⑥NE-1045

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－339045

(43)公開日　平成11年(1999)12月10日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６５Ｐ
Ｇ０６Ｆ　17/60		15/21	３４０Ｂ

審査請求　未請求　請求項の数11　ＯＬ　（全 34 頁）

(21)出願番号　特願平10－145910

(22)出願日　平成10年(1998)５月27日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　田坂　光伸
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所システム開発本部内
(72)発明者　高橋　英男
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所システム開発本部内
(72)発明者　増石　哲也
神奈川県横浜市都筑区加賀原二丁目２番
株式会社日立製作所システム開発本部内
(74)代理人　弁理士　秋田　収喜

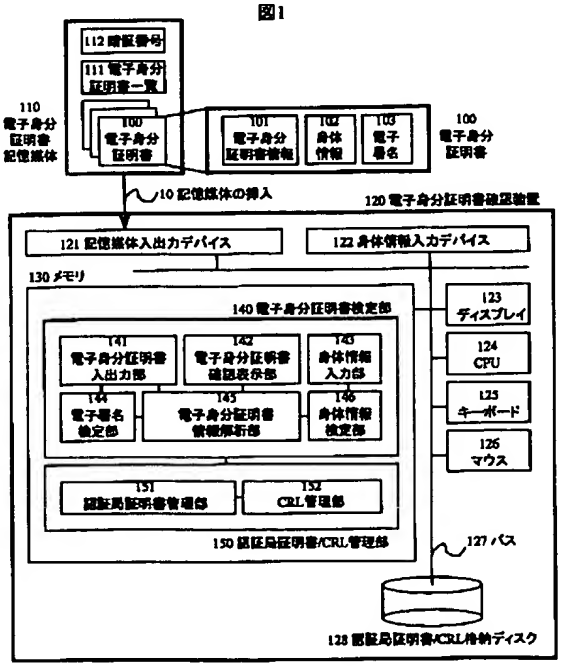
(54)【発明の名称】　電子データ確認及び発行方法、その実施装置、その処理プログラムを記録した媒体並びに電子データ記録媒体

(57)【要約】

【課題】　電子データ記録媒体に記録された電子データの不正使用を防止することが可能な技術を提供する。

【解決手段】　電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認方法において、電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定するステップと、当該電子データ記録媒体の保持者の身体情報を読み取り、読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定するステップとを有するものである。

図1



【特許請求の範囲】

【請求項１】　電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認方法において、

電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定するステップと、

当該電子データ記録媒体の保持者の身体情報を読み取り、読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定するステップとを有することを特徴とする電子データ確認方法。

【請求項２】　前記身体情報に対する電子署名を検定するステップは、前記電子データの発行機関である電子データ認証局の暗号鍵を用いて前記電子データの所有者の身体情報に対する電子署名を検定するものであることを特徴とする請求項１に記載された電子データ確認方法。

【請求項３】　前記身体情報に対する電子署名を検定するステップは、前記電子データの発行機関である電子データ認証局の暗号鍵に対する電子証明書が失効していないかを確認し、有効な電子証明書を用いて電子データ認証局の暗号鍵を検定し、前記検定が成功した暗号鍵を用いて前記身体情報に対する電子署名を検定するものであることを特徴とする請求項１に記載された電子データ確認方法。

【請求項４】　前記電子データ認証局とは別の機関が作成した任意の電子データに対する電子署名を検定するステップを有することを特徴とする請求項１乃至請求項３のいずれか１項に記載された電子データ確認方法。

【請求項５】　電子データを記録した電子データ記録媒体を発行する電子データ発行方法において、

電子データ記録媒体に記録される電子データの所有者の身体的特徴を示す身体情報を読み取り、前記身体情報に対する電子署名を作成するステップと、

前記電子データ、身体情報及びその電子署名を電子データ記録媒体に記録するステップとを備えることを特徴とする電子データ発行方法。

【請求項６】　前記電子データの発行機関である電子データ認証局とは別の機関が作成した任意の電子データと、前記任意の電子データに対する電子署名とを前記電子データ記録媒体に追加するステップを有することを特徴とする請求項５に記載された電子データ発行方法。

【請求項７】　電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認装置において、

電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定する電子署名検定部と、

当該電子データ記録媒体の保持者の身体情報を読み取る身体情報入力部と、前記身体情報入力部で読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定する身体情報検定部とを備えることを特徴とする電子データ確認装置。

【請求項８】　電子データを記録した電子データ記録媒体を発行する電子データ発行装置において、

電子データ記録媒体に記録される電子データの所有者の身体的特徴を示す身体情報を読み取る身体情報入力部と、前記身体情報に対する電子署名を作成する電子署名作成部と、

前記電子データ、身体情報及びその電子署名を有するデータを作成する電子データ作成部と、前記電子データ作成部により作成したデータを電子データ記録媒体に記録する電子データ入出力部とを備えることを特徴とする電子データ発行装置。

【請求項９】　電子データ記録媒体中に記録された電子データがその電子データ記録媒体を保持する保持者のものであるかどうかを確認する電子データ確認装置としてコンピュータを機能させる為のプログラムを記録した媒体において、

電子データ記録媒体に記録された電子データの所有者の身体的特徴を示す身体情報に対する電子署名を検定する電子署名検定部と、

当該電子データ記録媒体の保持者の身体情報を読み取る身体情報入力部と、前記身体情報入力部で読み取った保持者の身体情報と当該電子データの所有者の身体情報とが一致するかどうかを検定する身体情報検定部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする媒体。

【請求項１０】　電子データを記録した電子データ記録媒体を発行する電子データ発行装置としてコンピュータを機能させる為のプログラムを記録した媒体において、

電子データ記録媒体に記録される電子データの所有者の身体的特徴を示す身体情報を読み取る身体情報入力部と、前記身体情報に対する電子署名を作成する電子署名作成部と、

前記電子データ、身体情報及びその電子署名を有するデータを作成する電子データ作成部と、前記電子データ作成部により作成したデータを電子データ記録媒体に記録する電子データ入出力部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする媒体。

【請求項１１】　特定の所有者が所有する電子データを記録した電子データ記録媒体において、

その所有者が所有する電子データと、当該所有者の身体的特徴を示す身体情報と、当該身体情報の電子署名とを有するデータを記録したことを特徴とする電子データ記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は特定の人物に関する

情報を電子データとして発行し、その所有者の確認を行う電子データ処理システムに関し、特に人物の身分証明書をコンピュータが処理できる電子データとして実現し、当該身分証明書を発行したり、その保持者が所有者と一致するかを確認したりする電子データ処理システムに適用して有効な技術に関するものである。

【０００２】

【従来の技術】従来、身分証明書或いはそれに類似の個人情報を電子データとして実現することが広く行われている。なお本発明では、身分証明書の目的を以下の様に定義する。第一の目的は、身分証明書の保持者が身分証明書に記載された所有者本人であるかと、当該所有者が身分証明書の保証する資格を有していることを確認することである。第二の目的は、第一の目的事項の確認者が、身分証明書の保持者と対面している状態で、第一の目的事項を確認することである。

【０００３】身分証明書或いはそれに類似の個人情報を電子データとして実現する従来の技術はいくつか存在しており、例えば第一の公知例としては、International Telecommunication Union発行の「ITU-T Recommendation X.509 (1997), Information Technology - Open Systems Interconnection - The Directory:Authentication Framework」に記載されている。

【０００４】本公知例は、情報処理システムで用いられる暗号鍵の所有者が用いる電子証明書について記載しており、当該証明書は、証明書自体の識別番号、暗号鍵の所有者の名称、当該証明書の発行機関の名称、暗号鍵等の電子データと、その電子データに対する発行機関の電子署名とを格納している。

【０００５】本公知例の電子証明書は、コンピュータネットワークにおいて電子的な商取引を行う為のシステムに適用されており、例えばクレジットカードによる支払いをコンピュータネットワークにおいて行う為の通信手順を規定した「Secure Electronic Transaction Specification」(MasterCard International社及びVisa International社発行,1997)に述べられている様に、前記のデータのほか、郵便番号や住所等を示すデータを格納する。

【０００６】本公知例の電子証明書の主な目的は、ある情報処理システムにおいて、送信者と受信者が、互いの暗号鍵を交換するときに、受け取った暗号鍵が確かに相手のものであるかと、相手が当該情報処理システムに参加する資格を有しているかを確認することである。

【０００７】本公知例では、この様な確認処理は、先に述べた「電子証明書の発行機関の電子署名」により実現される。電子署名は、暗号技術を適用した情報処理システムで広く用いられているもので、電子署名の対象データの改竄の防止と電子署名の作成者の認証を達成する。電子署名については、例えばPrentice Hall社発行の「Network Security」(1995)に記載されている。

【０００８】電子署名は、本発明において重要な役割を果たすものであるので、ここで若干の説明を行う。

【０００９】電子署名を実現する技術として公開鍵暗号技術が広く用いられている。公開鍵暗号では二つの暗号鍵が登場する。これを暗号鍵ペアと呼ぶ。暗号鍵ペアの一方は秘密鍵と呼ばれ、その暗号鍵ペアの所有者が秘匿の責任を負う。他方は公開鍵と呼ばれ、例えば情報処理システムにおける通信相手に渡すものである。

【００１０】公開鍵暗号による電子署名は、以下の様に用いられる。以下では電子署名の作成者が、電子署名の検定者に渡したいデータのことを平文と呼ぶ。

【００１１】先ず作成者は平文を秘密鍵で暗号化する。この平文を暗号化することにより生成されたデータを暗文と呼ぶ。この暗文が「電子署名」である。作成者は、平文と暗文（電子署名）を検定者に渡す。この平文と暗文の組合せを、以降、「電子署名データ」と呼ぶ。

【００１２】次に検定者は、受け取った電子署名データの内、電子署名を作成者の公開鍵で復号する。作成者の公開鍵は、予め、または、電子署名データと共に、検定者に渡される。

【００１３】次に検定者は、平文と電子署名を復号することにより得られたデータを比較する。以下では、この比較において、互いが一致することを検定の成功と呼び、一致しないことを検定の失敗と呼ぶ。

【００１４】検定が成功したならば、以下のことがわかる。第一に、平文が改竄されていないことがわかる。平文を改竄すれば、電子署名の復号結果と一致しないからである。第二に、電子署名の作成者が、検定に用いた公開鍵と暗号鍵ペアを成す秘密鍵の所有者であることがわかる。何故なら、その公開鍵で復号できる暗文は、その公開鍵と暗号鍵ペアを成す秘密鍵で作成したものだけであることが、一般に公開鍵暗号アルゴリズムでは保証されているからである。

【００１５】ここで、電子署名の作成者の公開鍵がすりかえられていると、検定の成功は、前記の二つの事項を保証しないことになってしまう。公開鍵のすりかえを検出する為に用いられるのが、まさに、第一の公知例の電子証明書である。第一の公知例の電子証明書は、例えば公開鍵の所有者の名称や公開鍵を平文の一部とする電子署名データであり、電子証明書の電子署名の検定を行うことにより、公開鍵を含めた証明書データの改竄が検出できる。なお、以降では、電子署名の対象データである平文のことを「電子署名対象データ」と呼ぶ。

【００１６】第一の公知例の電子証明書は、その発行機関が、自らの秘密鍵により、電子証明書が含むデータに対して電子署名を施した電子署名データである。以下では、電子証明書の発行機関のことを認証局と呼ぶ。

【００１７】電子証明書を受け取った者は、当該認証局の公開鍵を入手し、当該電子証明書の電子署名を検定する。以下では、電子証明書の電子署名の検定のことを、

単に「電子証明書の検定」と呼ぶ。電子証明書の検定により、当該電子証明書が含むデータが改竄されていないことと、当該電子証明書が当該認証局から発行されたものであることを確認できる。

【００１８】ここで、電子証明書を検定する為に用いる認証局公開鍵がすりかわっていないことを保証する為に、更に電子証明書が用いられる。つまり、認証局の公開鍵は、電子証明書に格納されて配布される。第一の公知例では、認証局は階層的に構成されており、末端の暗号鍵所有者の電子証明書を発行する認証局自身の電子証明書は、更に上位の認証局が発行する。

【００１９】なお、第一の公知例では、効力を失った電子証明書を示す電子データが用いられている。この電子データは、CRL(Certificate Revocation List)と呼ばれるもので、効力を失った電子証明書の一覧を示すデータである。以降では、電子証明書が効力を失うことを「失効」と呼ぶ。第一の公知例では、CRLは、末端の暗号鍵所有者の電子証明書の失効だけでなく、認証局の電子証明書の失効も管理する。

【００２０】第二の公知例は、例えば特開平8-305766号公報「証明書自動交付機」に記載されている。本公知例は、住民票や印鑑証明書等の印刷物である証明書類の発行装置に関するもので、証明書の発行を申請する人が本人或いはその許可を得た人かどうかの確認を行う為のものである。本公知例では、ICカードに暗証番号と住民票や印鑑証明書等に記載されるべきデータを記憶する。証明書類の発行の際には、証明書自動交付機において、当該ICカードに記憶された暗証番号と発行申請者が入力する暗証番号を比較して本人確認を行う。

【００２１】なお、本公知例では、ICカードに記憶された住民票や印鑑証明書等のデータは、証明書自動交付機が住民票や印鑑証明書等の印刷物である証明書類を作成する為に用いられる。本公知例では、身分証明書はICカードそのものであり、その保持者が当該ICカードに記憶されたデータを印刷した証明書類を発行する資格を有していることを保証する。

【００２２】第三の公知例は、例えば特開平6-251049号公報「投票受付端末装置」に記載されている。本公知例は、選挙の投票受付端末装置に関するもので、投票を行う人（選挙人）が本人かどうかの確認を行う為のものである。本公知例では、選挙人が所有するICカードに当該選挙人の指紋の特徴データを記憶し、投票の際には、投票受付端末装置において当該ICカードに記憶された指紋と選挙人の指紋を比較して本人確認を行う。本公知例では、身分証明書はICカードそのものであり、その保持者が選挙権を有していることを保証する。

【００２３】第四の公知例は、現在、広く用いられているカード型や手帳型の印刷された身分証明書であり、例えばパスポート、運転免許証、社員証、学生証等である。この様な身分証明書は、一般に、その所有者が、ある資格を有していることを保証し、それぞれの資格の審査機関が発行する。

【００２４】

【発明が解決しようとする課題】人物が本人であるかと特定の資格を有しているかを確認する為の身分証明書を電子データとして実現しようとするとき、従来技術には以下の様な課題が存在する。

【００２５】第一の公知例の電子証明書は、盗まれてしまった場合に、不正使用が可能であるという問題がある。電子証明書は、通常、ICカード等の記憶媒体に記憶され、第三の公知例にも登場している様に、記憶媒体の記憶領域へのアクセスが暗証番号により保護されると考えられる。しかし、他人に記憶媒体を盗まれ、かつ、暗証番号を知られてしまうと、当該電子証明書は読み出し可能になってしまう。

【００２６】第一の公知例の電子証明書は認証局による電子署名データであり、当該電子証明書の検定者は、認証局の電子証明書を入手し、それが格納する認証局の公開鍵により、検定を行う。認証局電子証明書は、当該記憶媒体に格納されるか、検定者により、別途、入手されるものであるので、記憶媒体の暗証番号を看破されることにより、電子証明書の検定は成功してしまう。つまり、他人が盗んだ電子証明書の本人に成りすますことが可能になる。

【００２７】そもそも、第一の公知例は、コンピュータネットワークでの電子商取引システム等の公開鍵暗号技術を用いて送受信するメッセージの保護を行う様な情報処理システムへの適用を狙ったものであり、公開鍵暗号技術と共に用いなければ効力を発揮しえない。つまり、第一の公知例を適用した情報処理システムでは、電子証明書自体は公開のものであり、悪意を持った他人が入手したとしても、電子証明書が格納する公開鍵と暗号鍵ペアを成す秘密鍵を入手しない限り、不正使用はできない。その様な情報処理システムでは、電子証明書は、データの暗号や電子署名の検定に用いられるが、これらが可能であったとしても、相対するデータの復号や電子署名の作成ができなければ意味がない。

【００２８】第一の公知例を適用した情報処理システムでは、データの復号や電子署名の作成は、秘密鍵によってのみ行える様になっているので、第一の公知例の電子証明書は、それを適用した情報処理システムにおいては効力を発揮するのである。しかし、本発明が対象とする様な身分証明書としての使用は、第一の公知例の電子証明書が目的とするところではなく、効力を発揮しえない。

【００２９】第二の公知例の身分証明書は、ICカード自体である。ICカード自体が、住民票等の印刷された証明書類を自動交付機で交付してもらう資格を示す身分証明書となっている。第二の公知例の身分証明書には、以下の二つの課題がある。第一の課題は、ICカード自体が身

分証明書となっているため、個人が有する資格毎に身分証明書が必要となり、その保持の為に多くのスペースを必要とするということである。第二の課題は、ICカードを盗まれた場合に、不正使用が可能であるということである。第二の公知例では、これを暗証番号により防御しようとしているが、暗証番号を知られてしまった場合には、防御できない。

【００３０】第三の公知例の身分証明書は、ICカード自体である。ICカード自体が、選挙権を示す身分証明書になっている。第三の公知例には、以下の二つの課題がある。第一の課題は、ICカード自体が身分証明書となっているため、個人が有する資格毎に身分証明書が必要となり、その保持の為に多くのスペースを必要とするということである。第二の課題は、ICカードを盗まれた場合に、不正使用が可能であるということである。第三の公知例では、これを、当該ICカードの所有者の指紋データをICカードに格納し、当該指紋データをICカードの保持者の指紋と比較することにより防御しようとしている。しかし、ICカードを盗まれ、かつ、指紋データを偽造されてしまった場合には防御できない。また、同様のICカード自体を偽造することも可能と思われる。

【００３１】第四の公知例の身分証明書には、以下の三つの課題が存在する。第一の課題は、個人が有する資格毎に身分証明書が必要となるため、その保持の為に多くのスペースを必要とするということである。第二の課題は、身分証明書を盗まれた場合に、写真や発行機関の印鑑等の偽造を行うことにより、不正使用が可能ということである。第三の課題は、身分証明書の確認者が、身分証明書の発行機関の確認する手間や時間がかかるということである。身分証明書の発行機関が確認者にとって未知のものであった場合、発行機関の存在やその信頼性を確認する為には、例えば身分証明書に記載されている発行機関の電話番号へ電話したり、役所等のしかるべき第三者機関へ問い合わせる等を行わねばならない。手間や時間がかかるが故に、この手続きがおろそかになる可能性は大きく、結果として、偽造された身分証明書の不正使用が可能になる。また、既知の発行機関であっても、当該発行機関の印鑑等の偽造を行うことにより、当該発行機関が発行する身分証明書自体の偽造が可能と思われる。

【００３２】以上の様に、従来技術には、第一に身分証明書の携帯の為に多くのスペースを必要とすること、第二に身分証明書の不正使用が可能であること、第三に身分証明書の発行機関の信頼性の確認方法が確立されていない為に身分証明書の偽造が可能であること、といった課題がある。

【００３３】本発明の目的は上記問題を解決し、電子データ記録媒体に記録された電子データの不正使用を防止することが可能な技術を提供することにある。

【００３４】

【課題を解決するための手段】本発明は、電子データを記録した電子データ記録媒体を発行し、その所有者を確認する電子データ発行／確認方法において、当該電子データの所有者の身体情報及びその電子署名を有する電子データ記録媒体を発行し、その電子署名を検定して当該電子データの所有者を確認するものである。

【００３５】本発明では、例えば電子データを電子身分証明書情報とし、電子データ記録媒体を電子身分証明書記憶媒体とし、電子データの発行機関である電子データ認証局を電子身分証明書認証局として、電子身分証明書情報を記録したICカード等の電子身分証明書記憶媒体を発行する場合、まず電子身分証明書の所有者となる人物の身体的特徴を示す身体情報を入力する。

【００３６】次に前記入力した身体情報を電子身分証明書の発行機関である電子身分証明書認証局の暗号鍵で暗号化して当該身体情報に対する電子署名を作成した後、当該電子身分証明書の所有者の身分情報、前記作成した身体情報及びその電子署名を含む電子身分証明書を電子身分証明書記憶媒体に書き込む。

【００３７】電子身分証明書記憶媒体の保持者が電子身分証明書の所有者であるかどうかを確認する場合には、電子身分証明書中の身体情報に対する電子署名を検定し、前記身体情報の検定が成功した場合に、電子身分証明書記憶媒体の保持者の身体情報を読み取り、その読み取った身体情報が前記電子身分証明書の身体情報と一致するかどうかを検定する。

【００３８】本発明によれば、ある人物の身元や特定の資格を有しているかを確認する為の身分証明書等の各種情報を電子データとして実現できるので、単一の記録媒体に複数の身分証明書等の情報を格納することができ、複数の身分証明書の携帯に必要なスペースを削減することができる。

【００３９】また、本発明によれば、電子身分証明書にその所有者の身体情報とその身体情報に対する電子署名を含め、当該電子身分証明書の確認を行う際に、前記の所有者の身体情報に対する電子署名を検定し、当該電子身分証明書を保持する者の身体的特徴と前記の所有者の身体情報を比較することにより、当該電子身分証明書を保持する者が当該電子身分証明書の所有者であるかを確認することができる。たとえ、前記の電子身分証明書の所有者の身体情報が改竄されていたとしても、前記の所有者の身体情報に対する電子署名を検定することによりこれを検出することができるので、当該身分証明書の不正使用を防止することができる。

【００４０】また、本発明によれば、電子身分証明書の所有者の身体情報に対する電子署名を、電子身分証明書認証局がその暗号鍵を用いて作成した電子署名とすることができる。ここで、本発明によれば、電子身分証明書確認装置が、電子身分証明書認証局の暗号鍵の電子証明書である暗号鍵証明書を格納し、かつ、当該暗号鍵証明

書を検定できるので、電子身分証明書の所有者の身体情報に対する電子署名を検定する為の暗号鍵を電子身分証明書認証局の暗号鍵証明書に含めて電子身分証明書確認装置へ配布することができ、かつ、前記の電子身分証明書認証局の暗号鍵証明書の電子署名を検定することで、前記の電子身分証明書認証局の信頼性及び前記の電子身分証明書認証局の暗号鍵の信頼性を確認することができる。

【００４１】これにより、本発明によれば、電子身分証明書認証局の暗号鍵の偽造を防止することができ、電子身分証明書の偽造を防止することができる。また、電子身分証明書の確認者にとって未知の電子身分証明書認証局が発行したとされる電子身分証明書があったとしても、当該電子身分証明書認証局の信頼性を簡単に確認することができる。

【００４２】以上の様に本発明の電子データ処理システムによれば、電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【００４３】

【発明の実施の形態】（実施形態１）以下に所有者の身体的特徴を示す身体情報及びその電子署名により電子身分証明書の所有者を確認する実施形態１の電子データ処理システムについて説明する。

【００４４】実施形態１は、電子身分証明書情報を電子データとして記録する電子身分証明書記憶媒体と、その所有者の確認を行う電子身分証明書確認装置の動作を説明するものである。図１から図１１を用いて本実施形態を説明する。

【００４５】図１は本実施形態の電子身分証明書のデータ構造、電子身分証明書を記憶する記憶媒体及び電子身分証明書確認装置の概略構成を示す図である。図１に示す様に本実施形態の電子身分証明書確認装置１２０は、電子身分証明書入出力部１４１と、電子身分証明書確認表示部１４２と、身体情報入力部１４３と、電子署名検定部１４４と、電子身分証明書情報解析部１４５と、身体情報検定部１４６と、認証局証明書管理部１５１と、CRL管理部１５２とを有している。

【００４６】電子身分証明書入出力部１４１は記憶媒体入出力デバイス１２１を介して電子身分証明書記憶媒体１１０から、暗証番号１１２、電子身分証明書一覧１１１及び電子身分証明書１００を読み取る処理部である。

【００４７】電子身分証明書確認表示部１４２は電子身分証明書１００の内容をディスプレイ１２３に表示する処理部である。身体情報入力部１４３は身体情報入力デバイス１２２を介して電子身分証明書記憶媒体１１０の保持者の身体情報１０２ａを読み取る処理部である。

【００４８】電子署名検定部１４４は電子身分証明書１００の発行機関である電子身分証明書認証局の暗号鍵に対する暗号鍵証明書が失効していないかを確認し、有効な暗号鍵証明書を用いて電子身分証明書認証局の暗号鍵を検定し、前記検定が成功した暗号鍵を用いて、電子身分証明書記憶媒体１１０に記録された電子身分証明書１００の電子身分証明書認証局電子署名１０３を検定する処理部である。

【００４９】電子身分証明書情報解析部１４５は電子身分証明書１００の電子身分証明書情報１０１を解析する処理部である。身体情報検定部１４６は身体情報入力部１４３で読み取った電子身分証明書記憶媒体１１０の保持者の身体情報１０２ａが、電子身分証明書１００の所有者の身体情報１０２と一致するかどうかを検定する処理部である。

【００５０】認証局証明書管理部１５１は電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定に用いる電子身分証明書認証局の暗号鍵証明書を認証局証明書/CRL格納ディスク１２８を検索して取得する処理部である。CRL管理部１５２は失効した電子身分証明書１００や、電子身分証明書認証局の暗号鍵証明書を示すCRLを管理する処理部である。

【００５１】電子身分証明書確認装置１２０を電子身分証明書入出力部１４１、電子身分証明書確認表示部１４２、身体情報入力部１４３、電子署名検定部１４４、電子身分証明書情報解析部１４５、身体情報検定部１４６、認証局証明書管理部１５１及びCRL管理部１５２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はＣＤ－ＲＯＭ以外の他の媒体でも良い。

【００５２】電子身分証明書１００は、電子身分証明書情報１０１、身体情報１０２及び電子身分証明書認証局電子署名１０３を含む電子データである。

【００５３】電子身分証明書情報１０１は、当該電子身分証明書の所有者の氏名や所属等を示す身分情報や当該電子身分証明書の識別番号等の複数の電子データの集まりである。身体情報１０２は、当該電子身分証明書の所有者の身体的特徴を特定できるデータであり、例えば顔写真、指紋または声紋等を使用できる。また顔写真と身体的特徴を説明するテキストデータや、指紋と声紋等、複数の身体的特徴データを組合せたデータであっても良い。

【００５４】電子身分証明書認証局電子署名１０３は、電子身分証明書情報１０１と身体情報１０２を組み合わせたデータを電子署名データとする電子署名である。電子身分証明書認証局電子署名１０３は、当該電子身分証明書の発行機関である電子身分証明書認証局が作成するものである。

【００５５】電子身分証明書１００の所有者は、当該電

子身分証明書を電子身分証明書記憶媒体１１０に格納して携帯する。電子身分証明書記憶媒体１１０は、複数の電子身分証明書１００を格納しており、複数の電子身分証明書１００は、それぞれ異なる電子身分証明書認証局が発行したものである。

【００５６】ここで電子身分証明書記憶媒体１１０は、その所有者が所有する電子データである電子身分証明書情報１０１と、当該所有者の身体的特徴を示す身体情報１０２と、当該身体情報の電子身分証明書認証局電子署名１０３とを有するデータを記録したICカード等の電子データ記録媒体である。なお前記データを記録する記録媒体は、ICカード以外の他の媒体であっても良い。

【００５７】また電子身分証明書記憶媒体１１０は、電子身分証明書一覧１１１と暗証番号１１２を格納している。電子身分証明書一覧１１１は、電子身分証明書記憶媒体１１０が格納している電子身分証明書１００の一覧データある。暗証番号１１２は、電子身分証明書記憶媒体１１０から電子身分証明書１００等を読み取る際にチェックに用いられるデータである。

【００５８】電子身分証明書確認装置１２０は、電子身分証明書１００を用いて、ある人物の資格を確認する為の装置である。以下では、電子身分証明書確認装置１２０を使用し、電子身分証明書１００の保持者の資格を確認する人物のことを確認者と呼ぶ。また、ある時点で電子身分証明書１００が格納された電子身分証明書記憶媒体１１０を携帯している人物のことを当該電子身分証明書の保持者と呼ぶ。電子身分証明書確認装置１２０は、電子身分証明書１００の保持者が、確かに当該電子身分証明書の所有者であるかどうかという点と、確認者が確認したい資格を保有しているかという点を確認する為の装置である。

【００５９】電子身分証明書確認装置１２０は、以下の様な構造を有する。電子身分証明書確認装置１２０は、ディスプレイ１２３、CPU１２４、キーボード１２５、マウス１２６、メモリ１３０、バス１２７、記憶媒体入出力デバイス１２１、身体情報入力デバイス１２２、認証局証明書/CRL格納ディスク１２８から構成される。

【００６０】メモリ１３０には、電子身分証明書検定部１４０及び認証局証明書/CRL管理部１５０というプログラムが存在する。記憶媒体入出力デバイス１２１は、電子身分証明書記憶媒体１１０が格納する電子データを読み取るデバイスである。身体情報入力デバイス１２２は、電子身分証明書１００の保持者の身体情報１０２ａを入力するデバイスであり、例えば指紋入力デバイスや声紋入力デバイス等を使用することができる。

【００６１】電子身分証明書検定部１４０は、電子身分証明書１００の保持者が当該電子身分証明書の所有者であるかを検定する。電子身分証明書入出力部１４１は、記憶媒体入出力デバイス１２１を介して、電子身分証明書記憶媒体１１０から、暗証番号１１２、電子身分証明書一覧１１１、電子身分証明書１００を読み取る。電子身分証明書確認表示部１４２は、電子身分証明書１００の内容をディスプレイ１２３に表示する。

【００６２】身体情報入力部１４３は、身体情報入力デバイス１２２を介して、電子身分証明書１００の保持者の身体情報１０２ａを読み取る。電子署名検定部１４４は、電子身分証明書１００が失効していないかを確認し、電子身分証明書１００の電子身分証明書認証局電子署名１０３を検定する。電子身分証明書情報解析部１４５は、電子身分証明書１００の電子身分証明書情報１０１を解析する。身体情報検定部１４６は、身体情報入力部１４３が読み取った身体情報１０２ａが、電子身分証明書１００の身体情報１０２と一致するかどうかを検定する。

【００６３】認証局証明書/CRL格納ディスク１２８は、電子身分証明書認証局の暗号鍵証明書やCRL等を格納する。なおここでは暗号鍵の電子証明書のことを「暗号鍵証明書」と呼んでいる。

【００６４】認証局証明書/CRL管理部１５０は、電子身分証明書認証局の暗号鍵証明書やCRL等を管理する。認証局証明書管理部１５１は、電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定に用いる電子身分証明書認証局の暗号鍵証明書を認証局証明書/CRL格納ディスク１２８を検索して取得する。CRL管理部１５２は、CRLを認証局証明書/CRL格納ディスク１２８から検索する。電子身分証明書認証局の暗号鍵証明書とCRLについては、図２で詳しく説明する。

【００６５】図２は本実施形態の電子データ処理システムのシステム構成を示す図である。本実施形態は、電子身分証明書確認装置１２０、電子身分証明書認証局２０３、統括認証局２００から構成される。なお本実施形態において、複数の電子身分証明書確認装置１２０が存在しても良い。

【００６６】電子身分証明書認証局２０３は、電子身分証明書１００を発行する発行機関である電子データ認証局である。本実施形態では、電子身分証明書１００の種類毎に複数の電子身分証明書認証局２０３が存在する。

【００６７】統括認証局２００は、電子身分証明書認証局２０３の暗号鍵証明書の発行機関であり、電子身分証明書認証局２０３の権威を保証する。また統括認証局２００は、本実施形態で用いられる電子身分証明書１００及び電子身分証明書認証局証明書１８２の内、失効したものの一覧であるCRL１８４の発行機関でもある。

【００６８】電子身分証明書確認装置１２０の認証局証明書/CRL格納ディスク１２８には、電子身分証明書認証局証明書１８２、統括認証局公開鍵１８３、CRL１８４が格納される。

【００６９】電子身分証明書認証局証明書１８２は、電子身分証明書認証局２０３の暗号鍵証明書である。統括認証局公開鍵１８３は、統括認証局２００の公開鍵であ

る。CRL１８４は、失効した電子身分証明書１００及び失効した電子身分証明書認証局証明書１８２の一覧情報である。

【００７０】電子身分証明書認証局２０３は電子身分証明書認証局ディスク２０５を有する。電子身分証明書認証局ディスク２０５は、当該認証局の秘密鍵である電子身分証明書認証局秘密鍵２０４と、当該認証局の公開鍵の入った暗号鍵証明書である電子身分証明書認証局証明書１８２を格納している。

【００７１】統括認証局２００は、統括認証局ディスク２０２を有する。統括認証局ディスク２０２は、統括認証局２００の秘密鍵である統括認証局秘密鍵２０１と、統括認証局２００の公開鍵である統括認証局公開鍵１８３とCRL１８４を格納している。

【００７２】本実施形態において、電子身分証明書確認装置１２０は、電子身分証明書認証局証明書１８２、CRL１８４、統括認証局公開鍵１８３を以下の様に入手する。

【００７３】電子身分証明書認証局２０３は、統括認証局２００から新たな電子身分証明書認証局証明書１８２を入手すると、任意の記憶媒体に電子身分証明書認証局証明書１８２を格納し、電子身分証明書確認装置１２０に送付する。

【００７４】統括認証局２００は、新たなCRL１８４を作成すると、任意の記憶媒体に当該CRL１８４を格納し、電子身分証明書確認装置１２０に送付する。また統括認証局２００は、統括認証局公開鍵１８３を任意の記憶媒体に格納し、電子身分証明書確認装置１２０に送付する。

【００７５】次に図３を用いて、本実施形態の電子身分証明書１００及び電子身分証明書記憶媒体１１０の具体例を示す。

【００７６】図３は本実施形態の電子身分証明書認証局２０３の概念を示す図である。図３は、人物A３１１及び人物B３１２が複数の電子身分証明書認証局２０３から電子身分証明書１００の発行を受けている様子を示しており、本実施形態には、例えば電子身分証明書１００として、自動車の運転免許証１００１、パスポート１００２やA大学学生証１００４が存在する。

【００７７】それぞれの電子身分証明書認証局２０３として、運転免許証発行機関２０３１、パスポート発行機関２０３２、A大学学生証発行機関２０３３が存在する。

【００７８】人物A３１１は、自動車の運転資格と海外渡航資格を持っており、運転免許証発行機関２０３１から運転免許証１００１を、パスポート発行機関２０３２からパスポート１００２を、それぞれの発行機関において申請を行い発行してもらう（２１０）。

【００７９】同様に人物B３１２は、海外渡航資格を持っており、A大学の学生である。そこで人物B３１２は、パスポート発行機関２０３２からパスポート１００３を、A大学学生証発行機関２０３３からA大学学生証１００４を、それぞれの発行機関において申請を行って発行してもらう。

【００８０】人物A３１１及び人物B３１２は、それぞれ自らの電子身分証明書記憶媒体A１１０１、電子身分証明書記憶媒体B１１０２に、複数の電子身分証明書１００を格納して携帯する。ここで電子身分証明書確認装置１２０は、例えば出国審査機関に設置され、出国審査の際に電子身分証明書１００であるパスポート１００２を確認する為に用いられる。また電子身分証明書確認装置１２０は、例えば警察官によって携帯され、電子身分証明書１００である運転免許証１００１の確認の為に用いられる。

【００８１】この様に本実施形態によれば、身分証明書を電子データとして実現でき、複数種類の電子身分証明書１００を単一の電子身分証明書記憶媒体１１０に格納することができる。

【００８２】次に図４を用いて本実施形態における電子身分証明書１００、電子身分証明書認証局証明書１８２及びCRL１８４のデータ構造を説明する。

【００８３】図４は本実施形態の電子身分証明書１００、電子身分証明書認証局証明書１８２及びCRL１８４のデータ構造を示す図である。電子身分証明書１００は、電子身分証明書情報１０１、身体情報１０２、電子身分証明書認証局電子署名１０３から構成される。

【００８４】身体情報１０２については前述した。電子身分証明書認証局電子署名１０３は、電子身分証明書１００の発行機関である電子身分証明書認証局２０３が作成する電子署名である。この電子署名の電子署名対象データは、電子身分証明書情報１０１と身体情報１０２からなる複合データである。

【００８５】電子身分証明書情報１０１は、電子身分証明書ID１０１１、認証局証明書ID１０１２、身分情報１０１３から構成される。電子身分証明書ID１０１１は、電子身分証明書１００に付与された一意な番号である。認証局証明書ID１０１２は、当該電子身分証明書を発行した電子身分証明書認証局２０３の暗号鍵証明書である電子身分証明書認証局証明書１８２の一意な番号である。身分情報１０１３は、電子身分証明書１００の所有者の氏名、住所や所属等の身分を表す情報である。

【００８６】電子身分証明書認証局証明書１８２は、認証局証明書ID１８２１、電子身分証明書認証局公開鍵１８２３、統括認証局電子署名１８２４から構成されている。認証局証明書ID１８２１は、電子身分証明書認証局証明書１８２を識別する一意な番号である。電子身分証明書認証局公開鍵１８２３は、電子身分証明書認証局証明書１８２の所有者である電子身分証明書認証局２０３の公開鍵である。統括認証局電子署名１８２４は、電子身分証明書認証局証明書１８２の発行機関である統括認

証局２００が作成する電子署名である。この電子署名の電子署名対象データは、認証局証明書ID１８２１及び電子身分証明書認証局公開鍵１８２３から成る複合データである。

【００８７】CRL１８４は、効力を失った電子身分証明書１００及び電子身分証明書認証局証明書１８２の一覧データである。CRL１８４は、CRLID１８４１、電子身分証明書ID１８４２、認証局証明書ID１８４３、統括認証局電子署名１８４４から構成されている。

【００８８】CRLID１８４１は、CRL１８４を識別する為の一意な番号である。電子身分証明書ID１８４２は、失効した電子身分証明書１００の一意な番号であり、CRL１８４に複数エントリが存在する。認証局証明書ID１８４３は、失効した電子身分証明書認証局証明書１８２の一意な番号であり、CRL１８４に複数エントリが存在する。統括認証局電子署名１８４４は、CRL１８４の発行機関である統括認証局２００が作成する電子署名である。この電子署名の対象データは、CRLID１８４１、電子身分証明書ID１８４２、認証局証明書ID１８４３から成る複合データである。

【００８９】次に、図５、図６、図７を用いて、本実施形態における電子身分証明書１００及び電子身分証明書認証局証明書１８２の暗号技術を用いた確認の原理について説明する。これらの確認は電子署名を用いて行われるものである。本実施形態は、身体情報１０２と電子署名を併用することにより電子身分証明書１００を実現するものであり、ここで説明する原理は本発明の根幹を成す。

【００９０】先ず図５を用いて電子身分証明書１００の電子身分証明書認証局電子署名１０３の作成に関する原理について説明する。

【００９１】図５は本実施形態の電子身分証明書１００の作成の原理を示す図である。電子署名対象データ５０１は、電子身分証明書認証局電子署名１０３を作成する際の対象データである。電子署名対象データ５０１は、電子身分証明書情報１０１及び身体情報１０２から成る。

【００９２】電子身分証明書１００は、電子身分証明書情報１０１及び身体情報１０２を電子署名対象データ５０１から複写し（５０２）、電子身分証明書認証局電子署名１０３との複合データとすることにより作成される。電子身分証明書認証局電子署名１０３は、電子署名対象データ５０１を、電子身分証明書認証局秘密鍵２０４により暗号化したものである（５０３）。

【００９３】次に図６を用いて、電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定に関する原理について説明する。

【００９４】図６は本実施形態の電子身分証明書１００の確認の原理を示す図である。先ず、電子身分証明書１００の電子身分証明書情報１０１及び身体情報１０２を複写して電子署名対象データ６０１を作成する（６０２）。次に、電子身分証明書認証局電子署名１０３を電子身分証明書認証局公開鍵１８２３を用いて復号し、復号結果を電子署名対象データ６０１と比較して一致するかを調べる。この比較操作が、電子身分証明書認証局電子署名１０３の検定（６０３）である。

【００９５】本実施形態において、この検定操作は電子身分証明書確認装置１２０において行われており、電子身分証明書確認装置１２０は、電子身分証明書認証局公開鍵１８２３を電子身分証明書認証局証明書１８２から抽出して入手する。これにより、電子身分証明書１００の電子身分証明書情報１０１及び身体情報１０２に改竄がないことと、電子身分証明書１００の発行元が電子身分証明書認証局証明書１８２の所有者である電子身分証明書認証局２０３であることを確認できる。

【００９６】次に図７を用いて、電子身分証明書認証局証明書１８２の統括認証局電子署名１８２４の検定に関する原理について説明する。この統括認証局電子署名１８２４は、電子身分証明書認証局証明書１８２の発行機関である統括認証局２００が、統括認証局秘密鍵２０１を用いて作成したものである。

【００９７】図７は本実施形態の電子身分証明書認証局証明書１８２の確認の原理を示す図である。先ず、電子身分証明書認証局証明書１８２の認証局証明書ID１８２１及び電子身分証明書認証局公開鍵１８２３を複写して、電子署名対象データ７０１を作成する（７０２）。次に、統括認証局電子署名１８２４を統括認証局公開鍵１８３を用いて復号し、復号結果を電子署名対象データ７０１と比較して一致するかどうかを調べる。この比較操作が、統括認証局電子署名１８２４の検定（７０３）である。

【００９８】本実施形態では、この検定操作は電子身分証明書確認装置１２０において行われる。これにより、電子身分証明書認証局証明書１８２の認証局証明書ID１８４３及び電子身分証明書認証局公開鍵１８２３に改竄がないことと、電子身分証明書認証局証明書１８２の発行元が統括認証局２００であることを確認できる。

【００９９】次に図８から図１１を用いて、本実施形態における電子身分証明書確認装置１２０の動作の流れを説明する。

【０１００】図８は本実施形態の電子身分証明書一覧１１１の概要を示す図である。電子身分証明書一覧１１１は、電子身分証明書記憶媒体１１０に格納されている電子身分証明書１００の一覧である。電子身分証明書一覧１１１は、電子身分証明書１００のそれぞれに対応するエントリを有する。それぞれのエントリは、電子身分証明書ID１０１１、電子身分証明書種別８０２、電子身分証明書認証局名８０４から構成される。電子身分証明書ID１０１１は、当該電子身分証明書を識別する為の一意な番号である。電子身分証明書種別８０２は、当該電子

身分証明書がどの様な種類の身分証明書であるかを示す。電子身分証明書認証局名８０４は、当該電子身分証明書を発行した電子身分証明書認証局２０３の名称である。

【０１０１】次に図９を用いて、電子身分証明書確認装置１２０が電子身分証明書１００の確認を行う動作の流れを説明する。

【０１０２】図９は本実施形態の電子身分証明書確認装置１２０が電子身分証明書１００の確認を行う処理の処理手順を示すフローチャートである。先ず、電子身分証明書１００の保持者は、電子身分証明書記憶媒体１１０を記憶媒体入出力デバイス１２１に挿入する（９０２）。次に電子身分証明書１００の保持者は、キーボード１２５を介して電子身分証明書記憶媒体１１０の暗証番号１１２ａを入力する（９０４）。これは、電子身分証明書確認装置１２０が、電子身分証明書記憶媒体１１０の保持者がその所有者かどうかを確認するためである。

【０１０３】電子身分証明書検定部１４０は、これを受けて、入力された暗証番号１１２ａと電子身分証明書記憶媒体１１０の暗証番号１１２を比較する（９０６）。一致しなければ、電子身分証明書検定部１４０はディスプレイ１２３に電子身分証明書１００の確認が失敗したことを表示する（９１８）。一致すれば、電子身分証明書検定部１４０は、電子身分証明書一覧１１１の内容をディスプレイ１２３に表示する（９０８）。

【０１０４】次に確認者は、確認対象の電子身分証明書１００を選択し、それをキーボード１２５或いはマウス１２６を介して入力する（９０９）。次に電子身分証明書検定部１４０は、選択された電子身分証明書１００を電子身分証明書記憶媒体１１０から読み込み、電子身分証明書認証局電子署名１０３を検定する（９１０）。

【０１０５】検定が失敗すると、電子身分証明書検定部１４０はディスプレイ１２３に電子身分証明書１００の確認が失敗したことを表示する（９１８）。検定が成功すれば、電子身分証明書検定部１４０は、電子身分証明書１００の身分情報１０１３と身体情報１０２を抽出する（９１１）。検定が成功したことにより、電子身分証明書１００の電子身分証明書情報１０１の内容と身体情報１０２には改竄が無く、電子身分証明書認証局２０３が保証する内容が格納されていることが確認されたことになる。

【０１０６】次に電子身分証明書１００の保持者は、身体情報入力デバイス１２２を介して身体情報１０２ａを入力する（９１２）。例えば身体情報１０２として指紋が用いられる場合には指紋を、声紋が用いられる場合には声紋を入力する。

【０１０７】次に電子身分証明書検定部１４０は、入力された身体情報１０２ａと電子身分証明書１００の身体情報１０２を比較する（９１４）。一致しなければ、電子身分証明書検定部１４０はディスプレイ１２３に電子身分証明書１００の確認が失敗したことを表示する（９１８）。一致すれば、電子身分証明書検定部１４０は、ディスプレイ１２３に電子身分証明書１００の確認が成功したことと、身分情報１０１３の内容を表示する（９１６）。

【０１０８】身体情報１０２が入力された身体情報１０２ａと一致したことにより、電子身分証明書１００の保持者が、確かにその所有者であることが確認されたことになる。最後に確認者は、ディスプレイ１２３に表示された身分情報１０１３の内容が、自分の要求する資格を満たしているものかどうかを確認することになる。

【０１０９】ここで電子身分証明書記憶媒体１１０が、正式な所有者ではない他の人物Cにより保持されており、人物Cが暗証番号１１２を知ることができたという状況を考える。この様な場合であっても、本実施形態の電子身分証明書確認装置１２０は、人物Cが電子身分証明書１００の所有者でないことを検出することができる。この場合、ステップ９０６において、入力された暗証番号１１２ａと暗証番号１１２の比較は一致する。しかし、ステップ９１４において、入力された身体情報１０２ａと身体情報１０２の比較が失敗するため、電子身分証明書１００の確認は失敗する。

【０１１０】次に、電子身分証明書記憶媒体１１０が、正式な所有者ではない他の人物Cにより保持されており、人物Cが暗証番号１１２を知ることができ、かつ、人物Cが電子身分証明書１００の身体情報１０２を自分の身体情報１０２ａに入れ替えたという状況を考える。この様な場合であっても、本実施形態の電子身分証明書確認装置１２０は、人物Cが電子身分証明書１００の所有者でないことを検出することができる。

【０１１１】この場合、ステップ９０６において、入力された暗証番号１１２ａと暗証番号１１２の比較は成功する。また、ステップ９１４まで進んだとすると、入力された身体情報１０２ａと身体情報１０２の比較は成功してしまう。しかし、この場合には、ステップ９１０において、電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定が失敗する。何故なら、図６で説明した通り、人物Cの入れ替えた身体情報１０２ａが電子身分証明書１００の発行の際の電子身分証明書認証局電子署名１０３の作成に用いた身体情報１０２と異なっていると、電子署名検定（６０３）が失敗するからである。これにより、電子身分証明書１００の確認が失敗する。

【０１１２】この様に本実施形態によれば、電子身分証明書１００が他人により使用されたとしても、電子身分証明書確認装置１２０に入力された身体情報１０２ａと電子身分証明書１００の身体情報１０２を比較することにより、その事実を検出することができる。また、電子身分証明書１００の身体情報１０２が改竄されていたと

しても、電子身分証明書認証局電子署名１０３の検定により、その事実を検出することができる。

【０１１３】なお本実施形態では、身体情報検定部１４６が、電子身分証明書１００の身体情報１０２を、身体情報入力デバイス１２２を介して入力された電子身分証明書１００の保持者の身体情報１０２ａと比較する様にしたが、電子身分証明書確認表示部１４２が電子身分証明書１００の身体情報１０２の内容をディスプレイ１２３に表示し、確認者が前記のディスプレイ１２３に表示された内容を電子身分証明書１００の保持者の身体情報１０２ａと比較する様にしても良い。

【０１１４】次に図１０を用いて、図９のステップ９１０の動作を詳しく説明する。図１０は本実施形態の電子身分証明書１００の確認装置の動作の内、電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定処理の処理手順を示すフローチャートである。ステップ９１０は、電子身分証明書検定部１４０が電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定を行うものである。

【０１１５】電子身分証明書検定部１４０において、電子身分証明書入出力部１４１は、電子身分証明書１００を電子身分証明書記憶媒体１１０から読み取り、電子署名検定部１４４にその検定を要求する（９１０２）。

【０１１６】次に電子署名検定部１４４は、電子身分証明書１００の電子身分証明書情報１０１から認証局証明書ID１０１２を調べる（９１０４）。次に電子署名検定部１４４は、ステップ９１０４で読み出した認証局証明書ID１０１２を有する電子身分証明書認証局証明書１８２とCRL１８４を認証局証明書/CRL管理部１５０へ要求する（９１０６）。

【０１１７】認証局証明書/CRL管理部１５０は、電子署名検定部１４４から要求された電子身分証明書認証局証明書１８２とCRL１８４を検索する（９１０８）。本実施形態では、ステップ９１０８の動作は、認証局証明書/CRL格納ディスク１２８から電子身分証明書認証局証明書１８２とCRL１８４の検索として行われる。

【０１１８】ステップ９１０８で検索が失敗すると、電子署名検定部１４４は電子身分証明書入出力部１４１に検定失敗を応答する（９１４）。検索が成功すると、電子署名検定部１４４は、電子身分証明書１００の電子身分証明書ID１０１１がCRL１８４に記載されていないかを検査する（９１０９）。

【０１１９】記載があると、その電子身分証明書１００が失効しているということなので、電子署名検定部１４４は電子身分証明書入出力部１４１に検定失敗を応答する（９１１４）。記載がないと、電子署名検定部１４４は、電子身分証明書認証局証明書１８２の電子身分証明書認証局公開鍵１８２３を用いて、電子身分証明書１００の電子身分証明書認証局電子署名１０３を検定する（９１１０）。この手順の原理は、図６で説明した通りである。

【０１２０】検定が失敗すると、電子署名検定部１４４は電子身分証明書入出力部１４１に検定失敗を応答する（９１１２）。検定が成功すると、電子署名検定部１４４は電子身分証明書入出力部１４１に検定成功を応答する（９１１４）。なお、本実施形態において、電子身分証明書１００に有効期限を示すデータを設け、ステップ９１０の動作において有効期限を検査する様にしても良い。

【０１２１】次に図１１を用いて、電子身分証明書確認装置１２０が、電子身分証明書認証局証明書１８２とCRL１８４を入手する際の動作について述べる。

【０１２２】図１１は本実施形態の電子身分証明書確認装置１２０が電子身分証明書認証局証明書１８２とCRL１８４を入手する処理の処理手順を示すフローチャートである。図２の説明で述べた通り、電子身分証明書認証局２０３は、電子身分証明書認証局証明書１８２が更新されると、新たな電子身分証明書認証局証明書１８２を任意の記憶媒体に格納して電子身分証明書確認装置１２０へ送付する。

【０１２３】また統括認証局２００は、CRL１８４が更新されると、新たなCRL１８４を任意の記憶媒体に格納して電子身分証明書確認装置１２０へ送付する。ここで認証局証明書/CRL管理部１５０は、電子身分証明書認証局証明書１８２及びCRL１８４を前記の記憶媒体から入力する。

【０１２４】認証局証明書/CRL管理部１５０において、認証局証明書管理部１５１は、統括認証局公開鍵１８３を用いて電子身分証明書認証局証明書１８２の統括認証局電子署名１８２４を検定する（１１０４）。

【０１２５】ステップ１１０４の電子署名の検定の原理は、図７で説明した通りである。検定が失敗すると動作を終了する。検定が成功すると認証局証明書管理部１５１は、電子身分証明書認証局証明書１８２を認証局証明書/CRL格納ディスク１２８に格納する（１１０６）。

【０１２６】次にCRL管理部１５２は、認証局証明書/CRL格納ディスク１２８に格納されている統括認証局公開鍵１８３を用いて、CRL１８４の統括認証局電子署名１８４４を検定する（１１０８）。検定が失敗すると動作を終了する。検定が成功するとCRL管理部１５２は、CRL１８４を認証局証明書/CRL格納ディスク１２８に格納する（１１１０）。

【０１２７】次にCRL管理部１５２は、認証局証明書/CRL格納ディスク１２８に格納されている電子身分証明書認証局証明書１８２の認証局証明書ID１８２１が、CRL１８４に記載されているかを検査する（１１１２）。記載がなければ終了する。記載があれば、CRL管理部１５２は、CRL１８４に記載のあった電子身分証明書認証局証明書１８２を認証局証明書/CRL格納ディスク１２８から消去する（１１１４）。

【０１２８】この様に本実施形態では、図１１のステップ１１０４において、電子身分証明書認証局証明書１８２の統括認証局電子署名１８２４の検定が成功すれば、電子身分証明書１００の電子身分証明書認証局２０３が、確かな電子身分証明書１００の発行機関であると保証されていることがわかる。

【０１２９】電子身分証明書認証局証明書１８２は、ステップ１１０４の統括認証局電子署名１８２４の検定が成功しないかぎり、認証局証明書/CRL格納ディスク１２８には格納されえない。よって、確認者は、電子身分証明書確認装置１２０により電子身分証明書１００を確認する動作を行っている際、図１０のステップ９１０８において、電子身分証明書認証局証明書１８２の検索の成否により、電子身分証明書認証局２０３の権威が保証されているかどうかを知ることができる。

【０１３０】また逆に、統括認証局２００の認定を得ていない発行機関は、統括認証局電子署名１８２４の入った電子身分証明書認証局証明書１８２を所有することができない。よって、統括認証局２００の認定を得ていない発行機関が発行した電子身分証明書１００の保持者が現れたとしても、電子身分証明書確認装置１２０は、予め図１１のステップ１１０４において電子身分証明書認証局証明書１８２の統括認証局電子署名１８２４を検定することにより、その様な発行機関の電子身分証明書認証局証明書１８２を認証局証明書/CRL格納ディスク１２８から排除できるので、電子身分証明書１００が有効なものでないことを検出することができる。

【０１３１】この様に本実施形態によれば、電子身分証明書認証局証明書１８２を検定することにより、電子身分証明書認証局２０３の権威が保証されていることを簡単に確認することができる。また電子身分証明書認証局証明書１８２を検定することにより、電子身分証明書認証局証明書１８２及びそれが含む電子身分証明書認証局公開鍵１８２３が偽造されたことを検出できるので、電子身分証明書１００が偽造されていることを検出できる。

【０１３２】また本実施形態では、電子身分証明書確認装置１２０は、図１０のステップ９１０９により、電子身分証明書１００の発行後に資格が停止された人物の電子身分証明書１００や、電子身分証明書記憶媒体１１０の紛失時に当該電子身分証明書記憶媒体に格納されている電子身分証明書１００を、CRL１８４を用いて拒否することができる。

【０１３３】この様に本実施形態によれば、資格が停止された人物の電子身分証明書１００や紛失してしまった電子身分証明書１００を失効させ、その様な電子身分証明書１００の確認が成功してしまうことを防止することができる。

【０１３４】以上説明した様に本実施形態の電子データ処理システムによれば、電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【０１３５】（実施形態２）以下に電子身分証明書認証局証明書を通信ネットワークを介して入手する実施形態２の電子データ処理システムについて説明する。

【０１３６】実施形態１では、電子身分証明書確認装置１２０が電子身分証明書１００の確認の為の動作を行う際、電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２は、予め認証局証明書/CRL格納ディスク１２８に格納されていた。

【０１３７】これに対して本実施形態では、電子身分証明書確認装置１２０が電子身分証明書１００の確認の為の動作を行う際、認証局証明書/CRL格納ディスク１２８に電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２が無ければ、通信ネットワークを介して電子身分証明書認証局証明書１８２を入手する。

【０１３８】図１２は本実施形態の電子身分証明書１００のデータ構造、電子身分証明書１００を記憶する記憶媒体及びその確認装置の概要を示す図である。電子身分証明書１００、電子身分証明書記憶媒体１１０の構造は、実施形態１と同一である。電子身分証明書確認装置１２００は、電子身分証明書１００を確認する為の装置であり、実施形態１の電子身分証明書確認装置１２０とほぼ同一の構造を有する。以下、主に実施形態１と異なる点について説明する。

【０１３９】電子身分証明書確認装置１２００において、電子身分証明書検定部１４０は、実施形態１と同様の構造を有し同様に動作する。認証局証明書/CRL格納ディスク１２８は、実施形態１と同様に電子身分証明書認証局証明書１８２、統括認証局公開鍵１８３、CRL１８４を格納する。認証局証明書/CRL管理部１５０は、電子身分証明書認証局証明書１８２、CRL１８４を管理する。認証局証明書/CRL管理部１５０は、実施形態１とは異なり、認証局証明書管理サーバアクセス部１５３を有し、実施形態１と異なる動作を行うが、電子身分証明書検定部１４０との接続形態は実施形態１と同様である。

【０１４０】電子身分証明書確認装置１２００は、通信ネットワークコントローラ１６０を有し、通信ネットワーク１７０を介して認証局証明書管理サーバ１８０と接続されている。通信ネットワーク１７０は、有線ネットワークでも無線ネットワークでも良い。

【０１４１】認証局証明書管理サーバ１８０は、電子身分証明書認証局証明書１８２、CRL１８４を管理する。認証局証明書管理サーバ１８０は、認証局証明書管理サーバディスク１８１を持つ。認証局証明書管理サーバディスク１８１は、電子身分証明書認証局証明書１８２、CRL１８４を格納する。

【０１４２】認証局証明書/CRL管理部１５０において、

認証局証明書管理部１５１は、電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２を取得する。電子身分証明書認証局証明書１８２は、認証局証明書/CRL格納ディスク１２８を検索して取得されるか、或いは、認証局証明書管理サーバ１８０から取得されるか、或いは、取得できないかのいずれかである。CRL管理部１５２は、CRL１８４を認証局証明書/CRL格納ディスク１２８から検索する。

【０１４３】認証局証明書管理サーバアクセス部１５３は、認証局証明書管理サーバ１８０へ、通信ネットワーク１７０を介して、電子身分証明書認証局証明書１８２を要求する。認証局証明書管理サーバ１８０は、認証局証明書管理サーバディスク１８１を検索して、目的の電子身分証明書認証局証明書１８２があれば、それを通信ネットワーク１７０を介して返す。

【０１４４】図１３は本実施形態の電子データ処理システムのシステム構成を示す図である。通信ネットワーク１７０に、電子身分証明書確認装置１２００、認証局証明書管理サーバ１８０、電子身分証明書認証局２０３、統括認証局２００が接続されている。本実施形態では電子身分証明書１００の種類毎に複数の電子身分証明書認証局２０３が存在する。また本実施形態において、複数の電子身分証明書確認装置１２００が存在しても良い。

【０１４５】認証局証明書管理サーバ１８０は、電子身分証明書認証局証明書１８２、統括認証局公開鍵１８３、CRL１８４を、認証局証明書管理サーバディスク１８１に格納し、電子身分証明書確認装置１２００に供給する。

【０１４６】電子身分証明書認証局２０３は、統括認証局２００から新たな電子身分証明書認証局証明書１８２を取得すると、電子身分証明書認証局証明書１８２を認証局証明書管理サーバ１８０に通信ネットワーク１７０を介して渡す。認証局証明書管理サーバ１８０は、渡された電子身分証明書認証局証明書１８２を認証局証明書管理サーバディスク１８１に格納しておく。

【０１４７】また統括認証局２００は、CRL１８４が更新されると、それを、認証局証明書管理サーバ１８０に通信ネットワーク１７０を介して渡す。認証局証明書管理サーバ１８０は、渡されたCRL１８４を認証局証明書管理サーバディスク１８１に格納しておく。なお本実施形態において、複数の認証局証明書管理サーバ１８０を、例えば地域毎に設置しても構わない。

【０１４８】本実施形態において電子身分証明書確認装置１２００は、電子身分証明書認証局証明書１８２、CRL１８４、統括認証局公開鍵１８３を以下の様に入手する。

【０１４９】電子身分証明書確認装置１２００は、電子身分証明書１００の確認に必要な電子身分証明書認証局証明書１８２を通信ネットワーク１７０を介して認証局証明書管理サーバ１８０から入手する。

【０１５０】認証局証明書管理サーバ１８０は、新たなCRL１８４を入手すると、通信ネットワーク１７０を介して電子身分証明書確認装置１２００に送付する。また統括認証局２００は、統括認証局公開鍵１８３を任意の記憶媒体に格納し、電子身分証明書確認装置１２００に送付する。

【０１５１】次に図１４を用いて、本実施形態における電子身分証明書確認装置１２００の動作の流れを説明する。本実施形態において、電子身分証明書確認装置１２００の動作は、実施形態１の図９、図１０で説明した電子身分証明書確認装置１２０の動作と同様である。但し本実施形態においては、図１０のステップ９１０８の動作が実施形態１とは異なる。図１４は、本実施形態でのステップ９１０８の動作の詳細を説明するものである。

【０１５２】図１４は本実施形態の電子身分証明書確認装置１２００の処理手順を示すフローチャートである。ステップ９１０８で、認証局証明書/CRL管理部１５０は、電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定を行う際に用いる電子身分証明書認証局証明書１８２とCRL１８４を検索する。すなわち認証局証明書/CRL管理部１５０において、認証局証明書管理部１５１は、統括認証局公開鍵１８３とCRL１８４を、認証局証明書/CRL格納ディスク１２８から検索する（１４０２）。

【０１５３】次に、認証局証明書管理部１５１は、認証局証明書/CRL格納ディスク１２８から、認証局証明書ID１０１２を持つ電子身分証明書認証局証明書１８２を検索する（１４０４）。検索が成功すると、認証局証明書管理部１５１は、電子身分証明書認証局証明書１８２とCRL１８４を電子署名検定部１４４に返す（１４１８）。検索が失敗すると、認証局証明書管理部１５１は、認証局証明書管理サーバアクセス部１５３へ、認証局証明書ID１０１２を持つ電子身分証明書認証局証明書１８２を要求する（１４０６）。

【０１５４】次に、認証局証明書管理サーバアクセス部１５３は、通信ネットワークコントローラ１６０、通信ネットワーク１７０を介して、認証局証明書管理サーバ１８０に、認証局証明書ID１０１２を持つ電子身分証明書認証局証明書１８２を要求する（１４０８）。

【０１５５】次に、認証局証明書管理サーバ１８０は、認証局証明書管理サーバディスク１８１から、認証局証明書ID１０１２を持つ電子身分証明書認証局証明書１８２を検索する。検索成功なら電子身分証明書認証局証明書１８２を、認証局証明書管理サーバアクセス部１５３に返し、検索失敗ならその旨を示す応答を返す（１４１０）。検索失敗なら、認証局証明書管理部１５１は、検索失敗を示す応答を電子署名検定部１４４に返す（１４２０）。

【０１５６】検索成功であれば、認証局証明書管理部１５１は、電子身分証明書認証局証明書１８２の認証局証

明書ID１８２１がCRL１８４に記載されていないかを検査する（１４１２）。

【０１５７】記載がある場合には、認証局証明書管理部１５１は、検索失敗を示す応答を電子署名検定部１４４に返す（１４２０）。この場合、電子身分証明書認証局証明書１８２が失効していることになり、当該証明書の電子身分証明書認証局公開鍵１８２３により検定される電子身分証明書１００を有効でないとみなす。

【０１５８】ステップ１４１２で記載がない場合には、認証局証明書管理部１５１は、統括認証局公開鍵１８３を用いて、電子身分証明書認証局証明書１８２の統括認証局電子署名１８２４を検定する（１４１４）。この動作は、図７で説明した原理を用いて行われる。

【０１５９】検定失敗であれば、認証局証明書管理部１５１は、検索失敗を示す応答を電子署名検定部１４４に返す（１４２０）。検定成功であれば、認証局証明書管理部１５１は、電子身分証明書認証局証明書１８２を認証局証明書/CRL格納ディスク１２８に格納し（１４１６）、認証局証明書管理部１５１が電子身分証明書認証局証明書１８２とCRL１８４を電子署名検定部１４４に返す（１４１８）。

【０１６０】なお、本実施形態において、電子身分証明書確認装置１２００がCRL１８４を入手したときの動作は、実施形態１の図１１のステップ１１０８からステップ１１１４と同様に実施できる。

【０１６１】この様に本実施形態によれば、電子身分証明書確認装置１２００は、電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２を必要になったときに通信ネットワーク１７０を介して認証局証明書管理サーバ１８０から入手し、電子身分証明書認証局証明書１８２を検定することができる。

【０１６２】これにより、電子身分証明書確認装置１２００は、全ての電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２を予め認証局証明書/CRL格納ディスク１２８に格納しておく必要がなくなり、認証局証明書/CRL格納ディスク１２８の所要量や、電子身分証明書確認装置１２００の管理者が電子身分証明書認証局証明書１８２を入手する手間を低減することができる。

【０１６３】例えば電子身分証明書確認装置１２００の認証局証明書/CRL格納ディスク１２８には確認する頻度の高い電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２を格納しておき、その他の電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２は、電子身分証明書認証局２０３が発行した電子身分証明書１００を確認する必要が発生したときに、認証局証明書管理サーバ１８０から電子身分証明書認証局証明書１８２を入手する様にすることができる。

【０１６４】この様にしても、本実施形態によれば、電子身分証明書確認装置１２００が電子身分証明書認証局証明書１８２を入手した際に、電子身分証明書認証局証明書１８２を検定することにより、電子身分証明書認証局２０３の権威が保証されていることを簡単に確認することができる。

【０１６５】また、電子身分証明書認証局証明書１８２を検定することにより、電子身分証明書認証局証明書１８２及びそれが含む電子身分証明書認証局公開鍵１８２３が偽造されたことを検出できるので、電子身分証明書１００が偽造されていることを検出できる。

【０１６６】また、本実施形態によれば、電子身分証明書確認装置１２００はCRL１８４を通信ネットワーク１７０を介して認証局証明書管理サーバ１８０から入手することができるので、電子身分証明書確認装置１２００の管理者がCRL１８４を入手する手間を低減できる。

【０１６７】以上説明した様に本実施形態の電子データ処理システムによれば、電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【０１６８】（実施形態３）以下に所有者の身体的特徴を示す身体情報及びその電子署名を有する電子身分証明書の発行を行う実施形態３の電子データ処理システムについて説明する。

【０１６９】実施形態３は、電子身分証明書１００の発行装置の動作を説明する為のものであり、電子身分証明書１００を作成する手順を説明するものである。図１５及び図１６を用いて本実施形態を説明する。先ず図１５を用いて電子身分証明書１００の発行装置の構造について説明する。

【０１７０】図１５は本実施形態の電子身分証明書発行装置の概略構成を示す図である。図１５に示す様に本実施形態の電子身分証明書発行装置１２２０は、電子身分証明書入出力部１２４１と、電子身分証明書情報入力部１２４２と、身体情報入力部１２４３と、電子署名作成部１２４４と、電子身分証明書作成部１２４５とを有している。

【０１７１】電子身分証明書入出力部１２４１は記憶媒体入出力デバイス１２１を介して電子身分証明書記憶媒体１１０との間で入出力処理を行って、電子身分証明書作成部１２４５により作成された電子身分証明書１００を電子身分証明書記憶媒体１１０に書き込む処理部である。

【０１７２】電子身分証明書情報入力部１２４２は電子身分証明書情報１０１の身分情報１０１３を入力する処理部である。身体情報入力部１２４３は身体情報入力デバイス１２２を介して電子身分証明書情報１０１の所有者の身体情報１０２を読み取る処理部である。

【０１７３】電子署名作成部１２４４は電子身分証明書情報１０１及び身体情報１０２に対する電子身分証明書認証局電子署名１０３を作成する処理部である。電子身

分証明書作成部１２４５は電子身分証明書情報１０１、電子身分証明書情報１０１の所有者の身体情報１０２及びその電子身分証明書認証局電子署名１０３を有する電子身分証明書１００を作成する処理部である。

【０１７４】電子身分証明書発行装置１２２０を電子身分証明書入出力部１２４１、電子身分証明書情報入力部１２４２、身体情報入力部１２４３、電子署名作成部１２４４及び電子身分証明書作成部１２４５として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はＣＤ－ＲＯＭ以外の他の媒体でも良い。

【０１７５】本実施形態において、電子身分証明書発行装置１２２０は、電子身分証明書認証局２０３に設置される。電子身分証明書発行装置１２２０には、電子身分証明書認証局ディスク２０５が接続される。

【０１７６】電子身分証明書発行装置１２２０は、メモリ１３０に電子身分証明書発行部１２４０と認証局秘密鍵管理部１２５０なるプログラムを持つ。その他、電子身分証明書確認装置１２０と同様に、記憶媒体入出力デバイス１２１、身体情報入力デバイス１２２、ディスプレイ１２３、CPU１２４、キーボード１２５、マウス１２６を有する。

【０１７７】電子身分証明書発行部１２４０は、電子身分証明書１００の申請者の電子身分証明書１００を作成する。認証局秘密鍵管理部１２５０は、電子身分証明書１００の電子身分証明書認証局電子署名１０３を作成する為に用いる電子身分証明書認証局秘密鍵２０４を電子身分証明書認証局ディスク２０５から検索する。

【０１７８】次に図１６を用いて、電子身分証明書発行部１２４０の処理を説明する。なお本実施形態では、図１６の動作の事前に、電子身分証明書認証局２０３が申請者が電子身分証明書１００を所有するに足る資格を有しているかどうかの審査を終え、電子身分証明書１００の発行を認定しているものとする。

【０１７９】図１６は本実施形態の電子身分証明書発行部１２４０の処理手順を示すフローチャートである。図１６で先ず電子身分証明書１００の申請者は、電子身分証明書記憶媒体１１０を記憶媒体入出力デバイス１２１に挿入する（１３０２）。電子身分証明書１００の申請者が、キーボード１２５を介して電子身分証明書記憶媒体１１０の暗証番号１１２ａを入力する（１３０４）と、電子身分証明書入出力部１２４１は入力された暗証番号１１２ａと暗証番号１１２を比較する（１３０６）。

【０１８０】暗証番号１１２ａと暗証番号１１２とが一致しなければ、電子身分証明書１００の発行はできずに終了する。一致すれば、電子身分証明書１００の申請者はキーボード１２５またはマウス１２６を用いて電子身分証明書情報１０１の身分情報１０１３の為の情報を入力する（１３０８）。本実施形態において、この手順は電子身分証明書１００の発行者が行っても良い。

【０１８１】次に電子身分証明書発行部１２４０の電子身分証明書情報入力部１２４２は、入力された情報を受け取り、身分情報１０１３を作成する（１３１０）。

【０１８２】電子身分証明書１００の申請者は、身体情報入力デバイス１２２を用いて身体情報１０２の為の情報を入力し（１３１２）、身体情報入力部１２４３は、入力された情報を受け取り身体情報１０２を作成する（１３１４）。

【０１８３】電子身分証明書作成部１２４５は、電子身分証明書情報１０１の電子身分証明書ID１０１１を決定し、自らの電子身分証明書認証局証明書１８２の認証局証明書ID１８２１を調べ、電子身分証明書情報１０１を作成する（１３１６）。

【０１８４】電子署名作成部１２４４は、認証局秘密鍵管理部１２５０を介して、自らの電子身分証明書認証局秘密鍵２０４を電子身分証明書認証局ディスク２０５から読み込む（１３１８）。

【０１８５】次に電子署名作成部１２４４は、電子身分証明書情報１０１と身体情報１０２を電子署名対象データ５０１として、電子身分証明書認証局秘密鍵２０４を用いて電子身分証明書認証局電子署名１０３を作成する（１３２０）。

【０１８６】電子身分証明書作成部１２４５は、電子身分証明書情報１０１、身体情報１０２、電子身分証明書認証局電子署名１０３により、電子身分証明書１００を作成する（１３２２）。電子身分証明書入出力部１２４１は、電子身分証明書記憶媒体１１０に電子身分証明書１００を書き込む（１３２４）。最後に、電子身分証明書入出力部１２４１は、電子身分証明書一覧１１１に、当該電子身分証明書のエントリを追加する（１３２６）。

【０１８７】この様に本実施形態によれば、電子データとして実現した身分証明書であり、身体情報１０２と身体情報１０２に対する電子身分証明書認証局電子署名１０３を有する電子身分証明書１００を作成することができる。

【０１８８】（実施形態４）以下に所有者の身体的特徴を示す身体情報を圧縮・復元する実施形態４の電子データ処理システムについて説明する。

【０１８９】実施形態１では、電子身分証明書１００の身体情報１０２は、当該電子身分証明書の所有者の身体的特徴を示すデータそのものであった。本実施形態では、身体情報１０２を、当該電子身分証明書の所有者の身体的特徴を示すデータを圧縮したデータとする。

【０１９０】本実施形態では、電子身分証明書発行装置１２２０は、電子身分証明書１００の申請者が入力した身体情報を圧縮し、身体情報１０２に変換する処理部を有する。また電子身分証明書確認装置１２０は、電子身

分証明書１００の身体情報１０２を圧縮前の身体情報に復元する処理部を有する。

【０１９１】この様に本実施形態によれば、電子身分証明書１００のサイズを低減することができる。

【０１９２】（実施形態５）以下に所有者の身分情報を暗号化する実施形態５の電子データ処理システムについて説明する。

【０１９３】実施形態１では、電子身分証明書１００の身分情報１０１３は暗号化されていない。本実施形態では、身分情報１０１３を暗号化された電子データとする。

【０１９４】本実施形態では、電子身分証明書発行装置１２２０の電子身分証明書認証局ディスク２０５に身分情報１０１３を暗号化する為の暗号鍵を格納し、電子身分証明書発行装置１２２０が身分情報１０１３を暗号化する処理部を備える。

【０１９５】また、電子身分証明書確認装置１２０の認証局証明書/CRL格納ディスクに身分情報１０１３を復号する為の暗号鍵を格納し、電子身分証明書確認装置１２０が身分情報１０１３を復号する処理部を備える。

【０１９６】電子身分証明書確認装置１２０は、予め、身分情報１０１３を復号する為の暗号鍵を入手しておく。例えば統括認証局公開鍵１８３を入手する際に入手する。本実施形態では、身分情報１０１３を暗号化するとしたが、同様に、身体情報１０２を暗号化することもできる。

【０１９７】この様に本実施形態によれば、電子身分証明書１００の中の身分情報１０１３や身体情報１０２を秘匿することができる。

【０１９８】（実施形態６）以下に任意の情報及びその電子署名を追加する実施形態６の電子データ処理システムについて説明する。

【０１９９】本実施形態の電子身分証明書は、電子身分証明書の発行後に、当該電子身分証明書に任意の情報を追加できる様にし、かつ、追加した情報が確かであることを保証するものである。図１７及び図１８を用いて本実施形態を説明する。

【０２００】図１７は本実施形態の電子身分証明書の構造を示す図である。電子身分証明書１７００は、実施形態１の電子身分証明書１００と同様に、電子身分証明書情報１０１、身体情報１０２、電子身分証明書認証局電子署名１０３を有すると共に、追加情報証明書１７０２なる電子データを含む。

【０２０１】追加情報証明書１７０２は、電子身分証明書１７００の確認を行った際に電子身分証明書１７００へ追加する情報を保持し、かつ、その内容を保証する為の電子データである。

【０２０２】追加情報証明書１７０２は、認証局証明書ID１０１２、追加情報１７０４、追加情報認証局電子署名１７０６から構成される。

【０２０３】追加情報１７０４は、電子身分証明書情報１０１の発行機関である電子身分証明書認証局２０３とは別の機関が作成した任意の情報であり、電子身分証明書１７００の確認を行った際に電子身分証明書１７００へ追加される情報である。追加情報認証局電子署名１７０６は、追加情報１７０４を電子身分証明書１７００に追加する機関の秘密鍵によって作成される電子署名であり、追加情報１７０４を対象データとする電子署名である。認証局証明書ID１０１２は、追加情報１７０４を電子身分証明書１７００に追加する機関の暗号鍵証明書の一意な番号である。

【０２０４】本実施形態では、実施形態１の電子身分証明書確認装置１２０が設置される機関に、図１８の追加情報証明書発行装置が設置されているとする。本実施形態では、この様な機関を追加情報認証局と呼ぶ。図１８を用いて、追加情報証明書発行装置の構造と動作を説明する。

【０２０５】図１８は本実施形態の追加情報証明書発行装置の概略構成を示す図である。図１８に示す様に本実施形態の追加情報証明書発行装置１９２０は、追加情報証明書入出力部１９４１と、追加情報証明書情報入力部１９４２と、電子署名作成部１９４４と、追加情報証明書作成部１９４５とを有している。

【０２０６】追加情報証明書入出力部１９４１は電子身分証明書１７００に追加情報証明書１７０２を追加し電子身分証明書記憶媒体１１０に書き込む処理部である。追加情報証明書情報入力部１９４２はキーボード１２５やマウス１２６を介して入力される追加情報１７０４を受け取る処理部である。

【０２０７】電子署名作成部１９４４は追加情報１７０４に対する追加情報認証局電子署名１７０６を追加情報認証局秘密鍵１９６１により作成する処理部である。追加情報証明書作成部１９４５は追加情報認証局証明書１９６２の一意な番号と追加情報１７０４と作成した追加情報認証局電子署名１７０６を複合して追加情報証明書１７０２を作成する処理部である。

【０２０８】追加情報証明書発行装置１９２０を追加情報証明書入出力部１９４１、追加情報証明書情報入力部１９４２、電子署名作成部１９４４及び追加情報証明書作成部１９４５として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する媒体はＣＤ－ＲＯＭ以外の他の媒体でも良い。

【０２０９】追加情報証明書発行装置１９２０は、電子身分証明書確認装置１２０や電子身分証明書発行装置１２２０と同様に、記憶媒体入出力デバイス１２１、身体情報入力デバイス１２２、メモリ１３０、ディスプレイ１２３、CPU１２４、キーボード１２５、マウス１２６、バス１２７を備える。

【０２１０】また、メモリ１３０には、追加情報証明書発行部１９４０と認証局秘密鍵管理部１９５０というプログラムが存在する。また、追加情報認証局ディスク１９６０を備え、追加情報認証局ディスク１９６０には追加情報認証局秘密鍵１９６１と追加情報認証局証明書１９６２が格納されている。

【０２１１】追加情報認証局証明書１９６２は、追加情報認証局秘密鍵１９６１と暗号鍵ペアを成す公開鍵の暗号鍵証明書である。追加情報認証局証明書１９６２は、実施形態１の統括認証局２００と同様の機関から発行され、実施形態２の認証局証明書管理サーバ１８０と同様の機関に渡され保管されるとする。追加情報証明書発行部１９４０は、以下の様に動作する。

【０２１２】追加情報証明書情報入力部１９４２はキーボード１２５やマウス１２６を介して入力される追加情報１７０４を受け取り、電子署名作成部１９４４は追加情報１７０４に対する追加情報認証局電子署名１７０６を追加情報認証局秘密鍵１９６１により作成する。

【０２１３】追加情報証明書作成部１９４５は追加情報認証局証明書１９６２の一意な番号と追加情報１７０４と作成した追加情報認証局電子署名１７０６を複合して追加情報証明書１７０２を作成し、追加情報証明書入出力部１９４１が電子身分証明書１７００に追加情報証明書１７０２を追加し電子身分証明書記憶媒体１１０に書き込む。本実施形態では、追加情報１７０４にその発行機関の電子署名を施すことにより、追加情報１７０４の内容が確かであることを保証する。

【０２１４】本実施形態において、電子身分証明書１７００は、例えばパスポートである。この場合、追加情報１７０４は、例えば出国審査の証明情報であり、追加情報認証局電子署名１７０６は、例えば出国審査の証明印であると考えることができる。ここでは、出国審査機関を追加情報認証局と考えることができる。

【０２１５】出国審査機関には、電子身分証明書確認装置１２０と追加情報証明書発行装置１９２０が設置される。出国審査機関は、審査の申請者のパスポートである電子身分証明書１７００を実施形態１と同様に電子身分証明書確認装置１２０により確認した後、追加情報証明書発行装置１９２０により追加情報証明書１７０２を作成し、電子身分証明書１７００に追加する。

【０２１６】後で、他の機関が当該追加情報を確認する必要が発生した場合には、当該機関は、追加情報証明書１７０２の追加情報認証局電子署名１７０６を検定する。この検定操作に必要な追加情報認証局証明書１９６２は、実施形態１の認証局証明書管理サーバ１８０に類する機関から取得することができる。

【０２１７】この様に本実施形態によれば、電子身分証明書１７００が様々な機関により確認されるたびに、当該機関が内容を保証する情報を当該電子身分証明書１７００に追加し、後ほど電子身分証明書１７００の所有者が当該機関により保証される内容の情報を授与されていたかを確認することができる。

【０２１８】（実施形態７）以下に電子身分証明書の身体情報を別構造として記憶する実施形態７の電子データ記録媒体について説明する。

【０２１９】図１９は本実施形態の電子身分証明書及びその記憶媒体の概要を示す図である。本実施形態の電子身分証明書２０００は、電子身分証明書情報１０１と電子身分証明書認証局電子署名２００２から構成される。電子身分証明書２０００は、実施形態１の電子身分証明書１００と異なり、身体情報１０２を含まない。また電子身分証明書認証局電子署名２００２は、電子身分証明書情報１０１を対象データとする電子署名である。

【０２２０】一方本実施形態では、身体情報証明書２０２０を設ける。身体情報証明書２０２０は、身体情報１０２を含む電子データであり、身体情報１０２の内容を保証する為の電子データである。身体情報証明書２０２０は、実施形態１の電子身分証明書認証局２０３のいずれかが発行するものである。

【０２２１】身体情報証明書２０２０は、身体情報証明書情報２０２１、身体情報認証局電子署名２０２３から構成される。身体情報証明書情報２０２１は、身体情報証明書ID２０２２、認証局証明書ID１０１２、身体情報１０２から構成される。身体情報認証局電子署名２０２３は、身体情報証明書情報２０２１を対象データとする電子署名であり、実施形態１の電子身分証明書認証局２０３のいずれかが作成する。

【０２２２】身体情報証明書ID２０２２は、当該身体情報証明書の一意な番号である。認証局証明書ID１０１２は、身体情報認証局電子署名２０２３を作成した電子身分証明書認証局２０３の電子身分証明書認証局証明書１８２の一意な番号である。

【０２２３】本実施形態において、電子身分証明書記憶媒体２０１０は、電子身分証明書２０００を格納する記憶媒体である。電子身分証明書記憶媒体２０１０は、実施形態１の電子身分証明書記憶媒体１１０と同様に電子身分証明書一覧１１１、暗証番号１１２を格納する。また電子身分証明書記憶媒体２０１０は、身体情報証明書２０２０と電子身分証明書２０００を格納する。電子身分証明書記憶媒体２０１０は、単一の身体情報証明書２０２０と、複数の電子身分証明書２０００を格納する。

【０２２４】本実施形態では、電子身分証明書２０００を確認する為の装置は、実施形態１の電子身分証明書確認装置１２０と同様の構成を有する。但し、本実施形態において、電子身分証明書検定部１４０の電子署名検定部１４４は、電子身分証明書認証局電子署名２００２の検定と、身体情報認証局電子署名２０２３の検定を行う。身体情報検定部１４６は、身体情報証明書２０２０に入っている身体情報１０２を用いて、入力された身体情報１０２ａを検査する。

【０２２５】この様に本実施形態によれば、身体情報１０２が電子身分証明書２０００には含まれないので、電子身分証明書２０００のサイズを実施形態１の電子身分証明書１００に比べて低減できる。

【０２２６】

【発明の効果】本発明によれば電子データ記録媒体に記録された電子データの所有者の身体情報と、前記身体情報に対する電子署名により、当該電子データの不正使用を検出するので、電子データ記録媒体に記録された電子データの不正使用を防止することが可能である。

【図面の簡単な説明】

【図１】実施形態１の電子身分証明書のデータ構造、電子身分証明書を記憶する記憶媒体及び電子身分証明書確認装置の概略構成を示す図である。

【図２】実施形態１の電子データ処理システムのシステム構成を示す図である。

【図３】実施形態１の電子身分証明書認証局２０３の概念を示す図である。

【図４】実施形態１の電子身分証明書１００、電子身分証明書認証局証明書１８２及びCRL１８４のデータ構造を示す図である。

【図５】実施形態１の電子身分証明書１００の作成の原理を示す図である。

【図６】実施形態１の電子身分証明書１００の確認の原理を示す図である。

【図７】実施形態１の電子身分証明書認証局証明書１８２の確認の原理を示す図である。

【図８】実施形態１の電子身分証明書一覧１１１の概要を示す図である。

【図９】実施形態１の電子身分証明書確認装置１２０が電子身分証明書１００の確認を行う処理の処理手順を示すフローチャートである。

【図１０】実施形態１の電子身分証明書１００の確認装置の動作の内、電子身分証明書１００の電子身分証明書認証局電子署名１０３の検定処理の処理手順を示すフローチャートである。

【図１１】実施形態１の電子身分証明書確認装置１２０が電子身分証明書認証局証明書１８２とCRL１８４を入手する処理の処理手順を示すフローチャートである。

【図１２】実施形態２の電子身分証明書１００のデータ構造、電子身分証明書１００を記憶する記憶媒体及びその確認装置の概要を示す図である。

【図１３】実施形態２の電子データ処理システムのシステム構成を示す図である。

【図１４】実施形態２の電子身分証明書確認装置１２００の処理手順を示すフローチャートである。

【図１５】実施形態３の電子身分証明書発行装置の概略構成を示す図である。

【図１６】実施形態３の電子身分証明書発行部１２４０の処理手順を示すフローチャートである。

【図１７】実施形態６の電子身分証明書の構造を示す図である。

【図１８】実施形態６の追加情報証明書発行装置の概略構成を示す図である。

【図１９】実施形態７の電子身分証明書及びその記憶媒体の概要を示す図である。

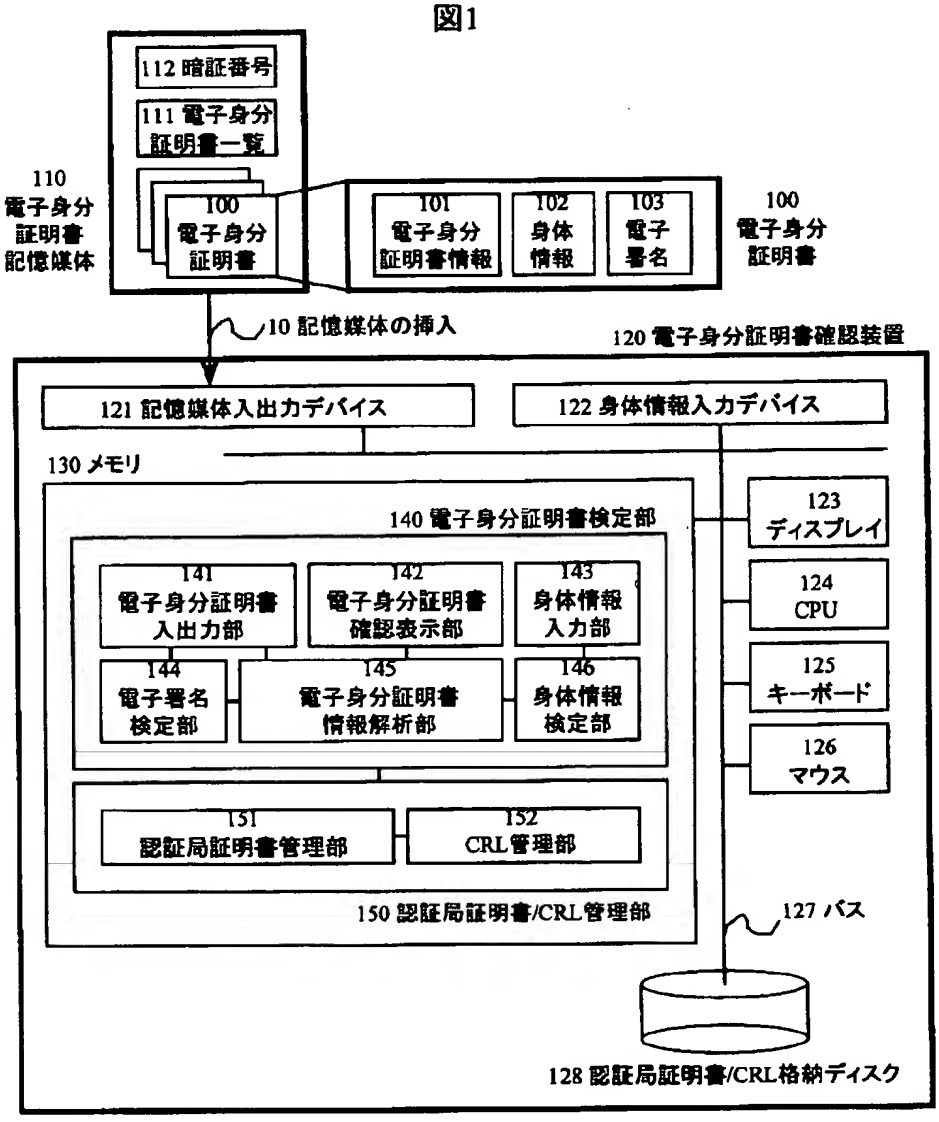
【符号の説明】

１００…電子身分証明書、１０１…電子身分証明書情報、１０２…身体情報、１０３…電子身分証明書認証局電子署名、１１０…電子身分証明書記憶媒体、１１１…電子身分証明書一覧、１１２…暗証番号、１２０…電子身分証明書確認装置、１２１…記憶媒体入出力デバイス、１２２…身体情報入力デバイス、１２３…ディスプレイ、１２４…CPU、１２５…キーボード、１２６…マウス、１２７…バス、１２８…認証局証明書/CRL格納ディスク、１３０…メモリ、１４０…電子身分証明書検定部、１５０…認証局証明書/CRL管理部、１４１…電子身分証明書入出力部、１４２…電子身分証明書確認表示部、１４３…身体情報入力部、１４４…電子署名検定部、１４５…電子身分証明書情報解析部、１４６…身体情報検定部、１５１…認証局証明書管理部、１５２…CRL管理部、１８２…電子身分証明書認証局証明書、１８３…統括認証局公開鍵、１８４…CRL、２００…統括認証局、２０１…統括認証局秘密鍵、２０２…統括認証局ディスク、２０３…電子身分証明書認証局、２０４…電子身分証明書認証局秘密鍵、２０５…電子身分証明書認証局ディスク、３１１…人物A、３１２…人物B、１００１…運転免許証、１００２…パスポート、１００３…パスポート、１００４…A大学学生証、１１０１…電子身分証明書記憶媒体A、１１０２…電子身分証明書記憶媒体B、２０３１…運転免許証発行機関、２０３２…パスポート発行機関、２０３３…A大学学生証発行機関、１０１１…電子身分証明書ID、１０１２…認証局証明書ID、１０１３…身分情報、１８２１…認証局証明書ID、１８２３…電子身分証明書認証局公開鍵、１８２４…統括認証局電子署名、１８４１…CRLID、１８４２…電子身分証明書ID、１８４３…認証局証明書ID、１８４４…統括認証局電子署名、５０１…電子署名対象データ、６０１…電子署名対象データ、７０１…電子署名対象データ、８０２…電子身分証明書種別、８０４…電子身分証明書認証局名、１２００…電子身分証明書確認装置、１５３…認証局証明書管理サーバアクセス部、１６０…通信ネットワークコントローラ、１７０…通信ネットワーク、１８０…認証局証明書管理サーバ、１８１…認証局証明書管理サーバディスク、１２２０…電子身分証明書発行装置、１２４０…電子身分証明書発行部、１２５０…認証局秘密鍵管理部、１２４１…電子身分証明書入出力部、１２４２…電子身分証明書情報入力部、１２４３…身体情報入力部、１２４４…電子署名作成部、１２４５…電子身分証明書作成部、１７００…電子身分証明

書、１７０２…追加情報証明書、１７０４…追加情報、１７０６…追加情報認証局電子署名、１９２０…追加情報証明書発行装置、１９４０…追加情報証明書発行部、１９５０…認証局秘密鍵管理部、１９６０…追加情報認証局ディスク、１９６１…追加情報認証局秘密鍵、１９６２…追加情報認証局証明書、１９４１…追加情報証明書入出力部、１９４２…追加情報証明書情報入力部、１９４４…電子署名作成部、１９４５…追加情報証明書作成部、２０００…電子身分証明書、２００２…電子身分証明書認証局電子署名、２０１０…電子身分証明書記憶媒体、２０２０…身体情報証明書、２０２１…身体情報証明書情報、２０２２…身体情報証明書ID、２０２３…身体情報認証局電子署名。

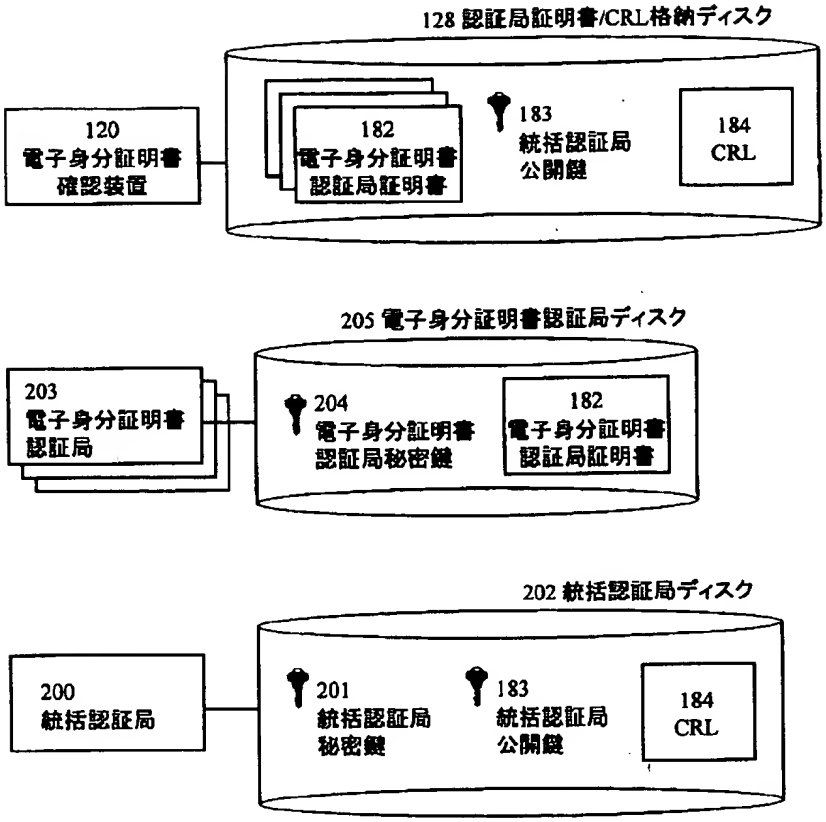
【図１】

図1



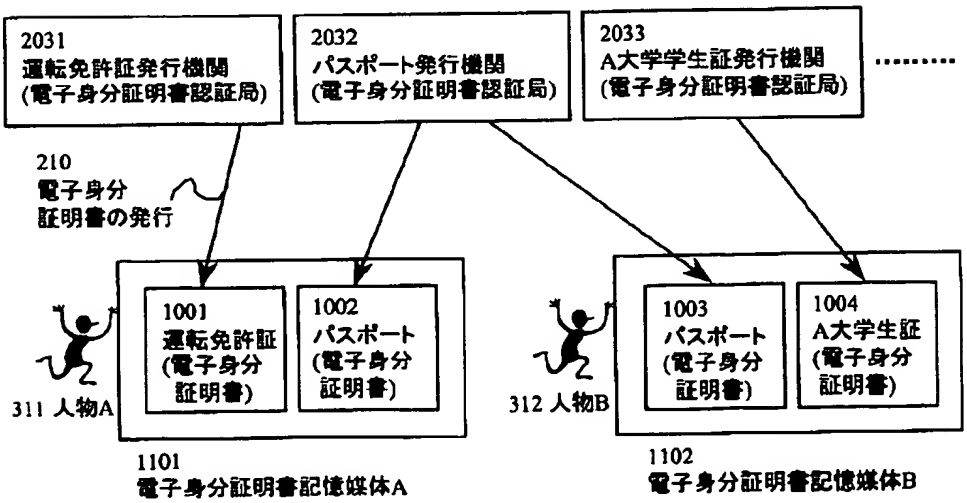
【図２】

図2


128 認証局証明書/CRL格納ディスク
120
電子身分証明書
確認装置
182
電子身分証明書
認証局証明書
183
統括認証局
公開鍵
184
CRL
205 電子身分証明書認証局ディスク
203
電子身分証明書
認証局
204
電子身分証明書
認証局秘密鍵
182
電子身分証明書
認証局証明書
202 統括認証局ディスク
200
統括認証局
201
統括認証局
秘密鍵
183
統括認証局
公開鍵
184
CRL

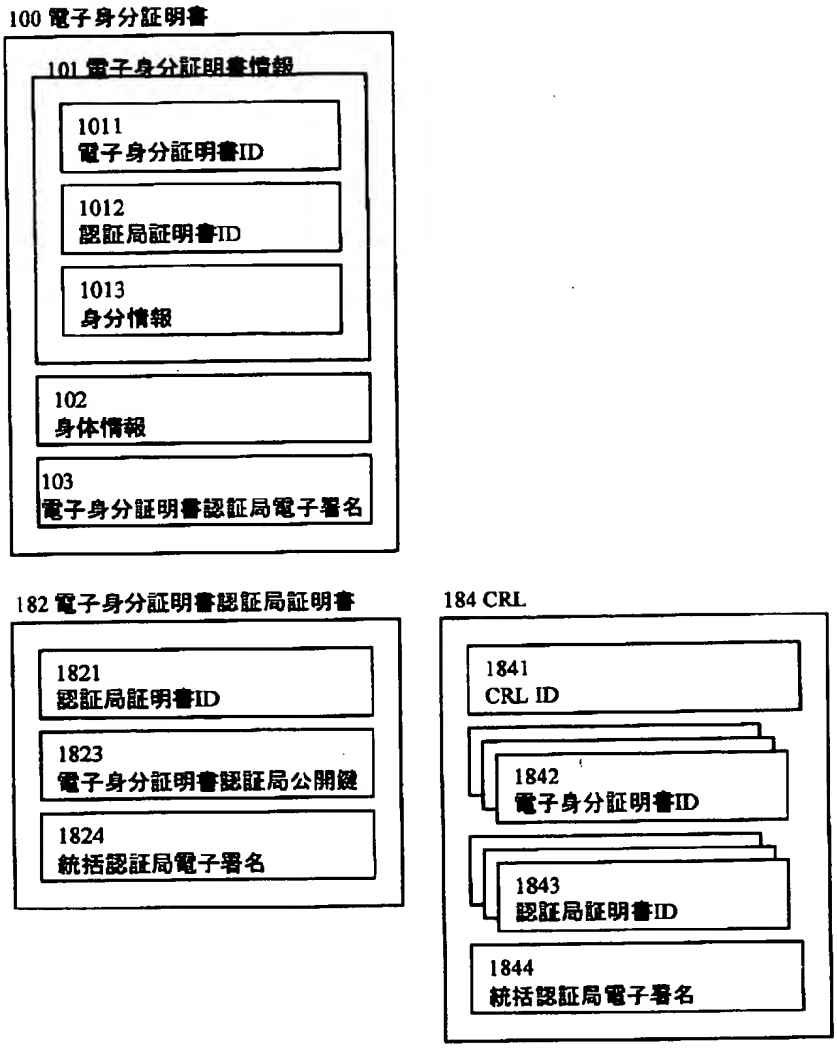
【図３】

図3


2031
運転免許証発行機関
(電子身分証明書認証局)
2032
パスポート発行機関
(電子身分証明書認証局)
2033
A大学学生証発行機関
(電子身分証明書認証局)
210
電子身分
証明書の発行
311 人物A
1001
運転免許証
(電子身分
証明書)
1002
パスポート
(電子身分
証明書)
1101
電子身分証明書記憶媒体A
312 人物B
1003
パスポート
(電子身分
証明書)
1004
A大学生証
(電子身分
証明書)
1102
電子身分証明書記憶媒体B

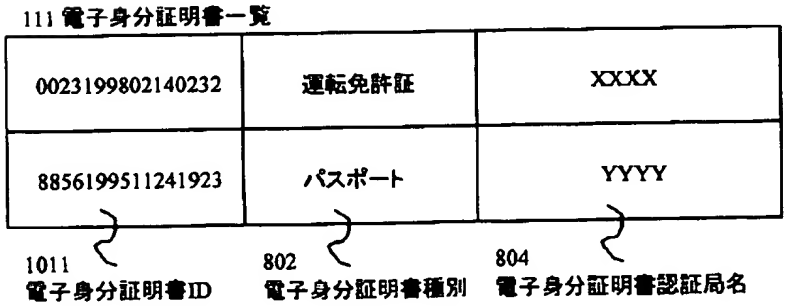
【図４】

図4


100 電子身分証明書
101 電子身分証明書情報
1011
電子身分証明書ID
1012
認証局証明書ID
1013
身分情報
102
身体情報
103
電子身分証明書認証局電子署名
182 電子身分証明書認証局証明書
1821
認証局証明書ID
1823
電子身分証明書認証局公開鍵
1824
統括認証局電子署名
184 CRL
1841
CRL ID
1842
電子身分証明書ID
1843
認証局証明書ID
1844
統括認証局電子署名

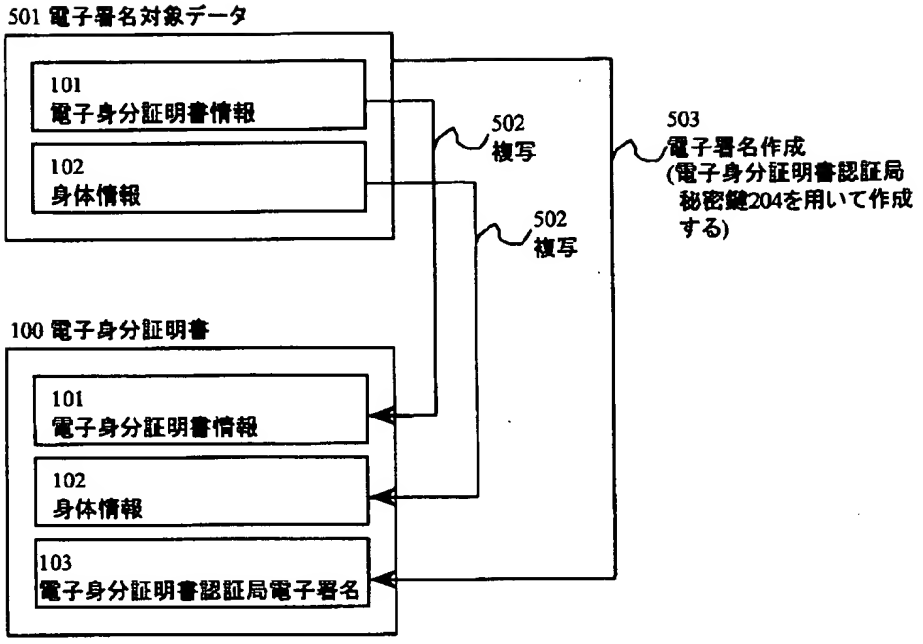
【図８】

図8


111 電子身分証明書一覧
0023199802140232
運転免許証
XXXX
8856199511241923
パスポート
YYYY
1011
電子身分証明書ID
802
電子身分証明書種別
804
電子身分証明書認証局名

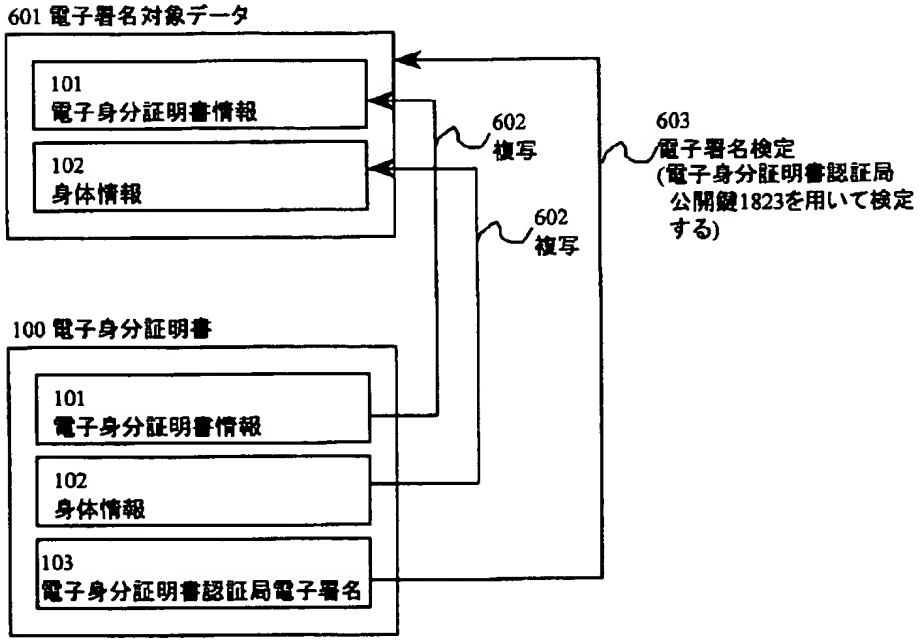
【図５】

図5


501 電子署名対象データ
101
電子身分証明書情報
102
身体情報
502
複写
502
複写
503
電子署名作成
(電子身分証明書認証局
秘密鍵204を用いて作成
する)
100 電子身分証明書
101
電子身分証明書情報
102
身体情報
103
電子身分証明書認証局電子署名

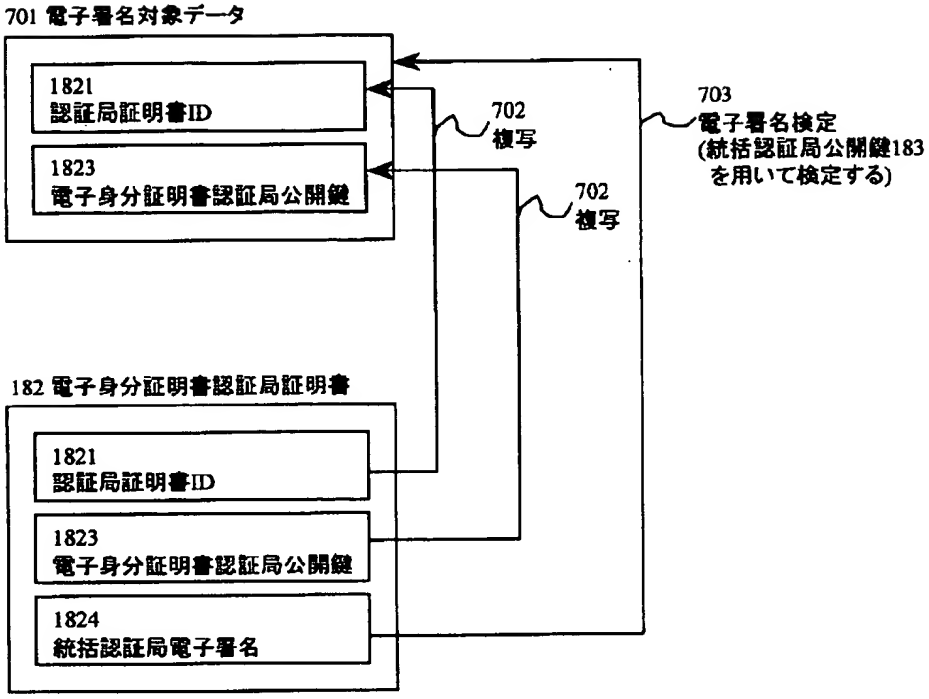
【図６】

図6


601 電子署名対象データ
101
電子身分証明書情報
102
身体情報
602
複写
602
複写
603
電子署名検定
(電子身分証明書認証局
公開鍵1823を用いて検定
する)
100 電子身分証明書
101
電子身分証明書情報
102
身体情報
103
電子身分証明書認証局電子署名

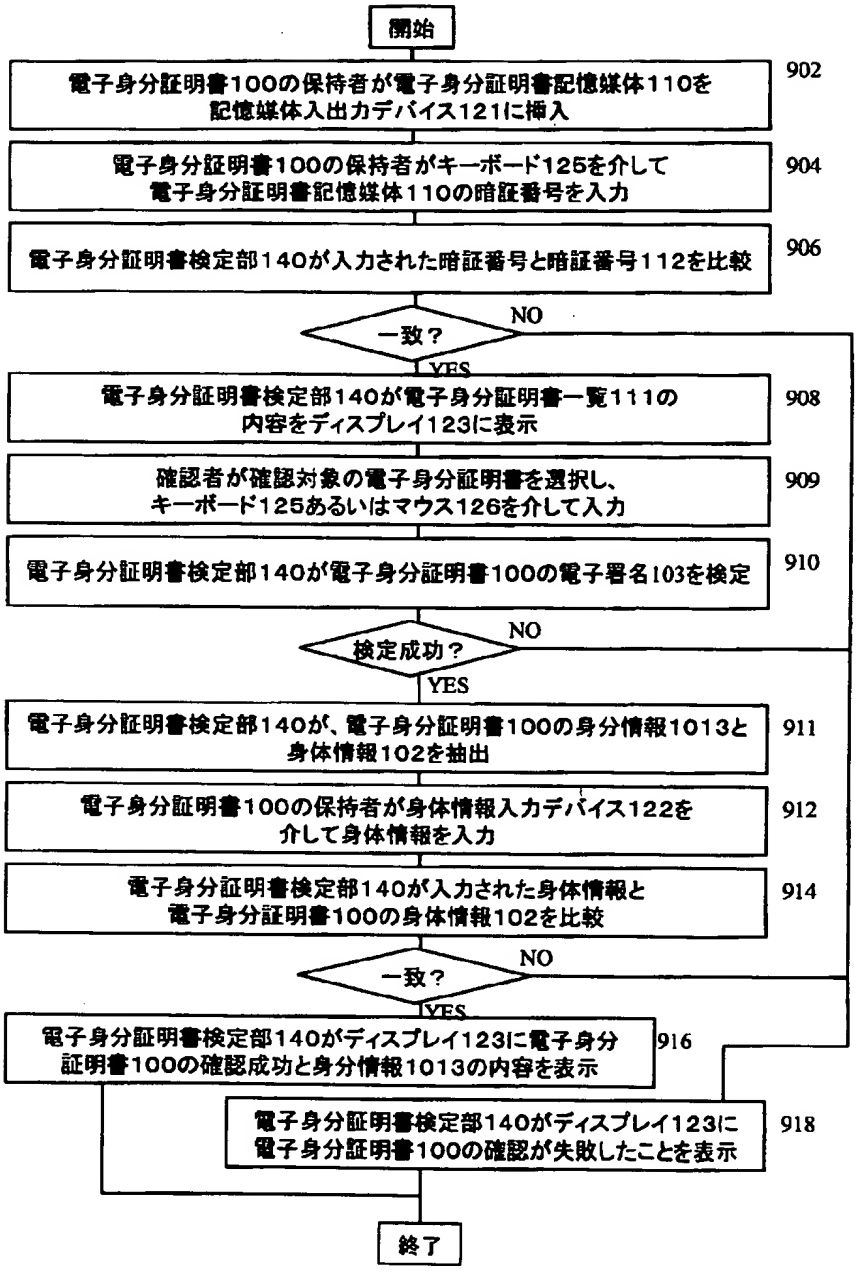
【図７】

図7


701 電子署名対象データ
1821
認証局証明書ID
1823
電子身分証明書認証局公開鍵
702
複写
702
複写
703
電子署名検定
(統括認証局公開鍵183
を用いて検定する)
182 電子身分証明書認証局証明書
1821
認証局証明書ID
1823
電子身分証明書認証局公開鍵
1824
統括認証局電子署名

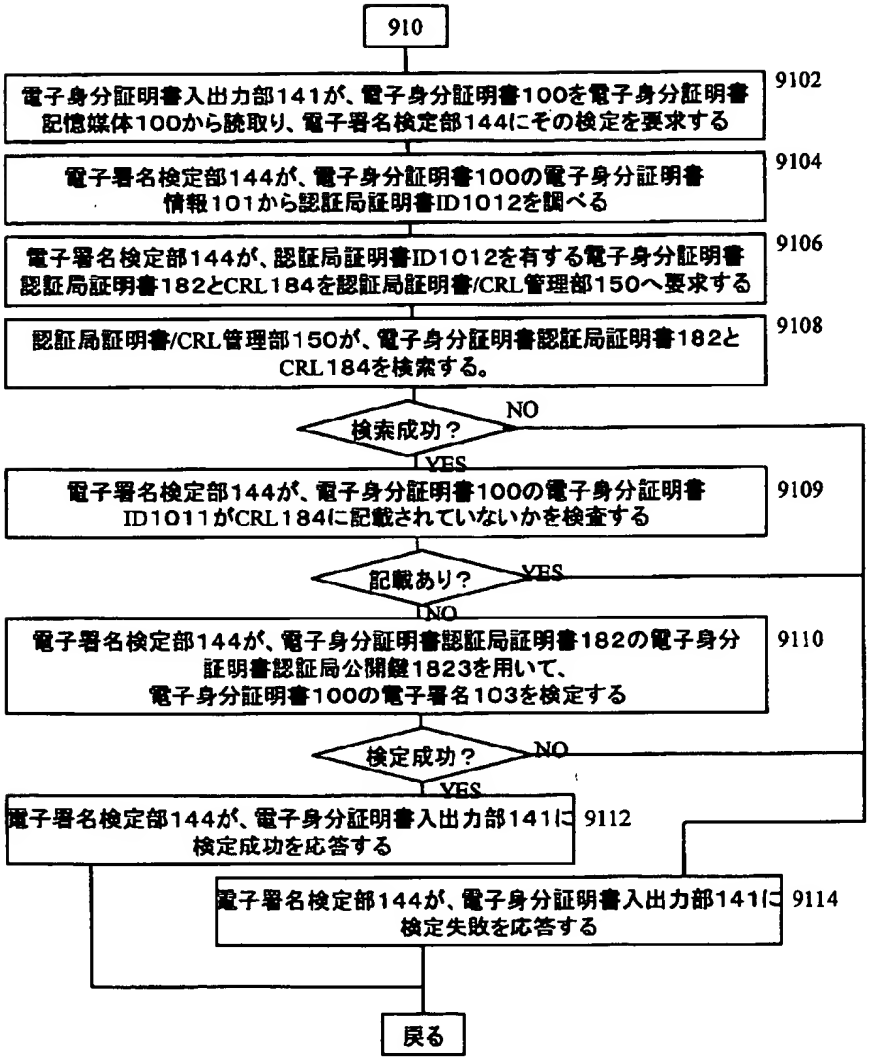
【図９】

図9


開始
電子身分証明書100の保持者が電子身分証明書記憶媒体110を記憶媒体入出力デバイス121に挿入
902
電子身分証明書100の保持者がキーボード125を介して電子身分証明書記憶媒体110の暗証番号を入力
904
電子身分証明書検定部140が入力された暗証番号と暗証番号112を比較
906
一致？
NO
YES
電子身分証明書検定部140が電子身分証明書一覧111の内容をディスプレイ123に表示
908
確認者が確認対象の電子身分証明書を選択し、キーボード125あるいはマウス126を介して入力
909
電子身分証明書検定部140が電子身分証明書100の電子署名103を検定
910
検定成功？
NO
YES
電子身分証明書検定部140が、電子身分証明書100の身分情報1013と身体情報102を抽出
911
電子身分証明書100の保持者が身体情報入力デバイス122を介して身体情報を入力
912
電子身分証明書検定部140が入力された身体情報と電子身分証明書100の身体情報102を比較
914
一致？
NO
YES
電子身分証明書検定部140がディスプレイ123に電子身分証明書100の確認成功と身分情報1013の内容を表示
916
電子身分証明書検定部140がディスプレイ123に電子身分証明書100の確認が失敗したことを表示
918
終了

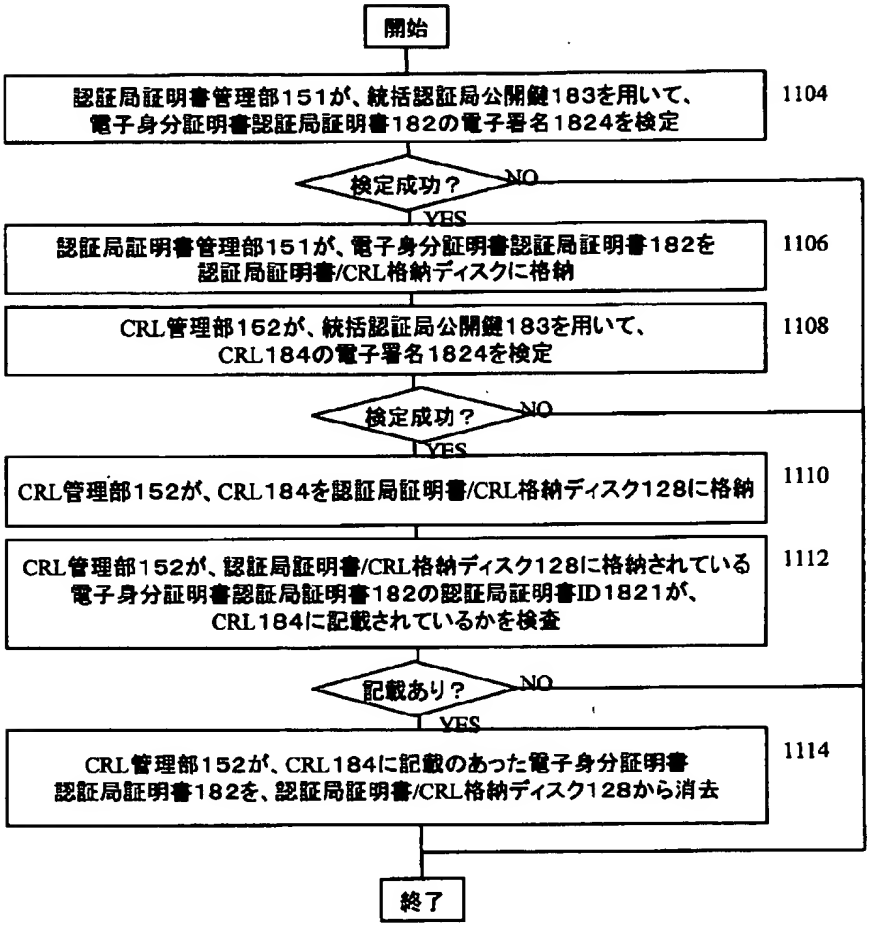
【図１０】

図10


910
電子身分証明書入出力部141が、電子身分証明書100を電子身分証明書記憶媒体100から読取り、電子署名検定部144にその検定を要求する
9102
電子署名検定部144が、電子身分証明書100の電子身分証明書情報101から認証局証明書ID1012を調べる
9104
電子署名検定部144が、認証局証明書ID1012を有する電子身分証明書認証局証明書182とCRL184を認証局証明書/CRL管理部150へ要求する
9106
認証局証明書/CRL管理部150が、電子身分証明書認証局証明書182とCRL184を検索する。
9108
検索成功？
NO
YES
電子署名検定部144が、電子身分証明書100の電子身分証明書ID1011がCRL184に記載されていないかを検査する
9109
記載あり？
YES
NO
電子署名検定部144が、電子身分証明書認証局証明書182の電子身分証明書認証局公開鍵1823を用いて、電子身分証明書100の電子署名103を検定する
9110
検定成功？
NO
YES
電子署名検定部144が、電子身分証明書入出力部141に検定成功を応答する
9112
電子署名検定部144が、電子身分証明書入出力部141に検定失敗を応答する
9114
戻る

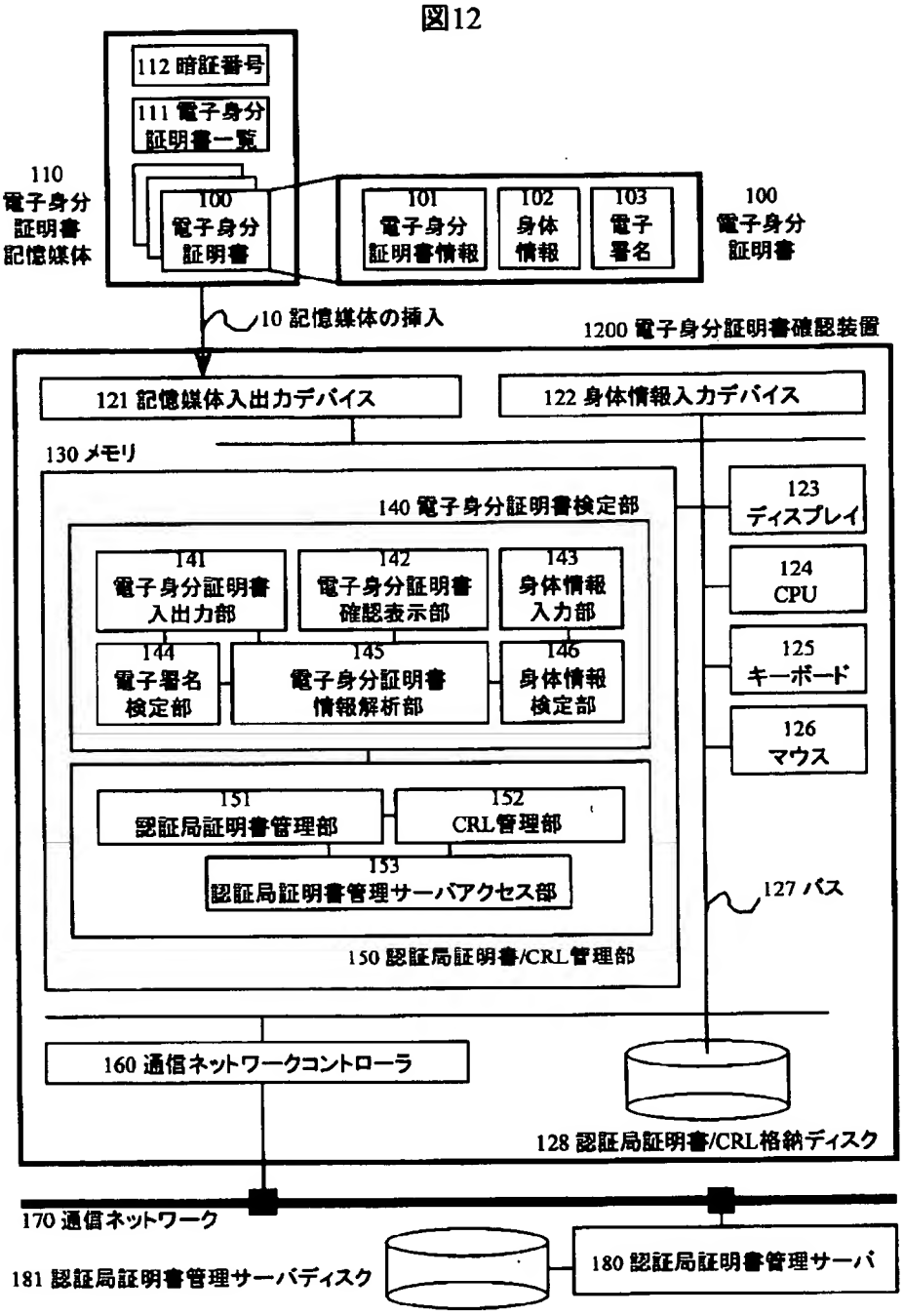
【図１１】

図11


開始
認証局証明書管理部151が、統括認証局公開鍵183を用いて、電子身分証明書認証局証明書182の電子署名1824を検定
1104
検定成功？
NO
YES
認証局証明書管理部151が、電子身分証明書認証局証明書182を認証局証明書/CRL格納ディスクに格納
1106
CRL管理部152が、統括認証局公開鍵183を用いて、CRL184の電子署名1824を検定
1108
検定成功？
NO
YES
CRL管理部152が、CRL184を認証局証明書/CRL格納ディスク128に格納
1110
CRL管理部152が、認証局証明書/CRL格納ディスク128に格納されている電子身分証明書認証局証明書182の認証局証明書ID1821が、CRL184に記載されているかを検査
1112
記載あり？
NO
YES
CRL管理部152が、CRL184に記載のあった電子身分証明書認証局証明書182を、認証局証明書/CRL格納ディスク128から消去
1114
終了

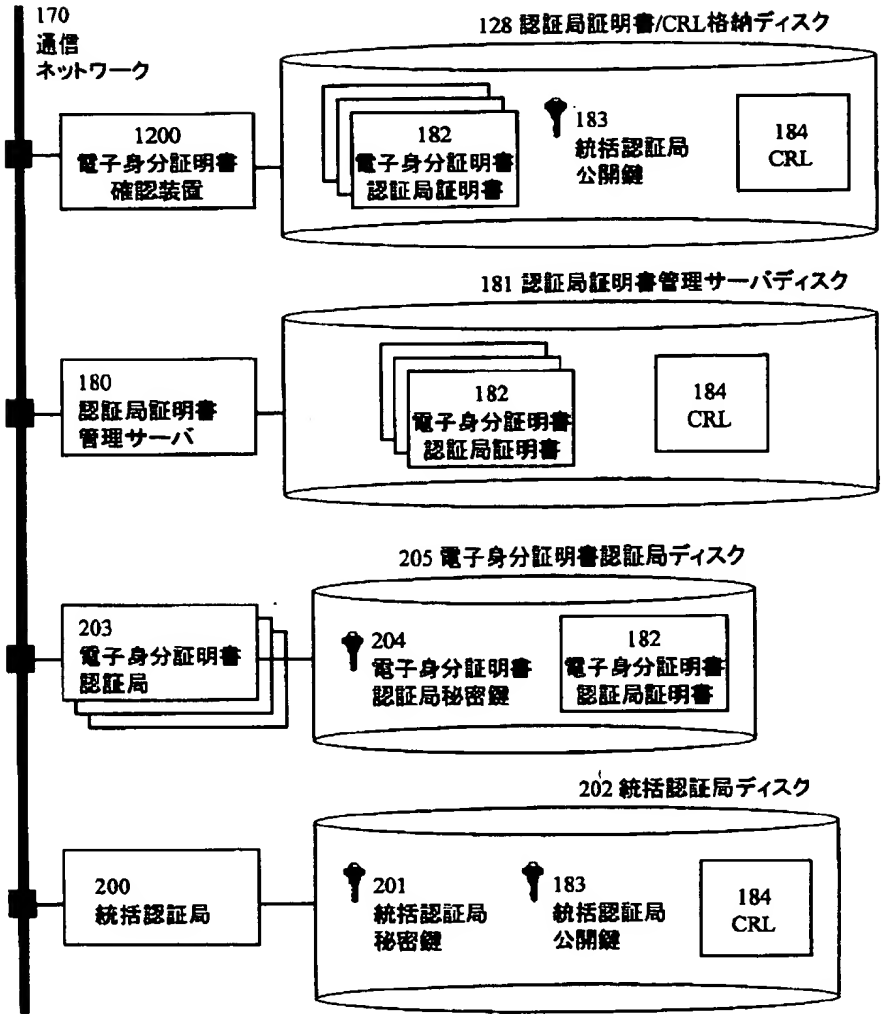
【図１２】

図12


112 暗証番号
111 電子身分証明書一覧
110 電子身分証明書記憶媒体
100 電子身分証明書
101 電子身分証明書情報
102 身体情報
103 電子署名
100 電子身分証明書
10 記憶媒体の挿入
1200 電子身分証明書確認装置
121 記憶媒体入出力デバイス
122 身体情報入力デバイス
130 メモリ
140 電子身分証明書検定部
141 電子身分証明書入出力部
142 電子身分証明書確認表示部
143 身体情報入力部
144 電子署名検定部
145 電子身分証明書情報解析部
146 身体情報検定部
150 認証局証明書/CRL管理部
151 認証局証明書管理部
152 CRL管理部
153 認証局証明書管理サーバアクセス部
123 ディスプレイ
124 CPU
125 キーボード
126 マウス
127 バス
160 通信ネットワークコントローラ
128 認証局証明書/CRL格納ディスク
170 通信ネットワーク
181 認証局証明書管理サーバディスク
180 認証局証明書管理サーバ

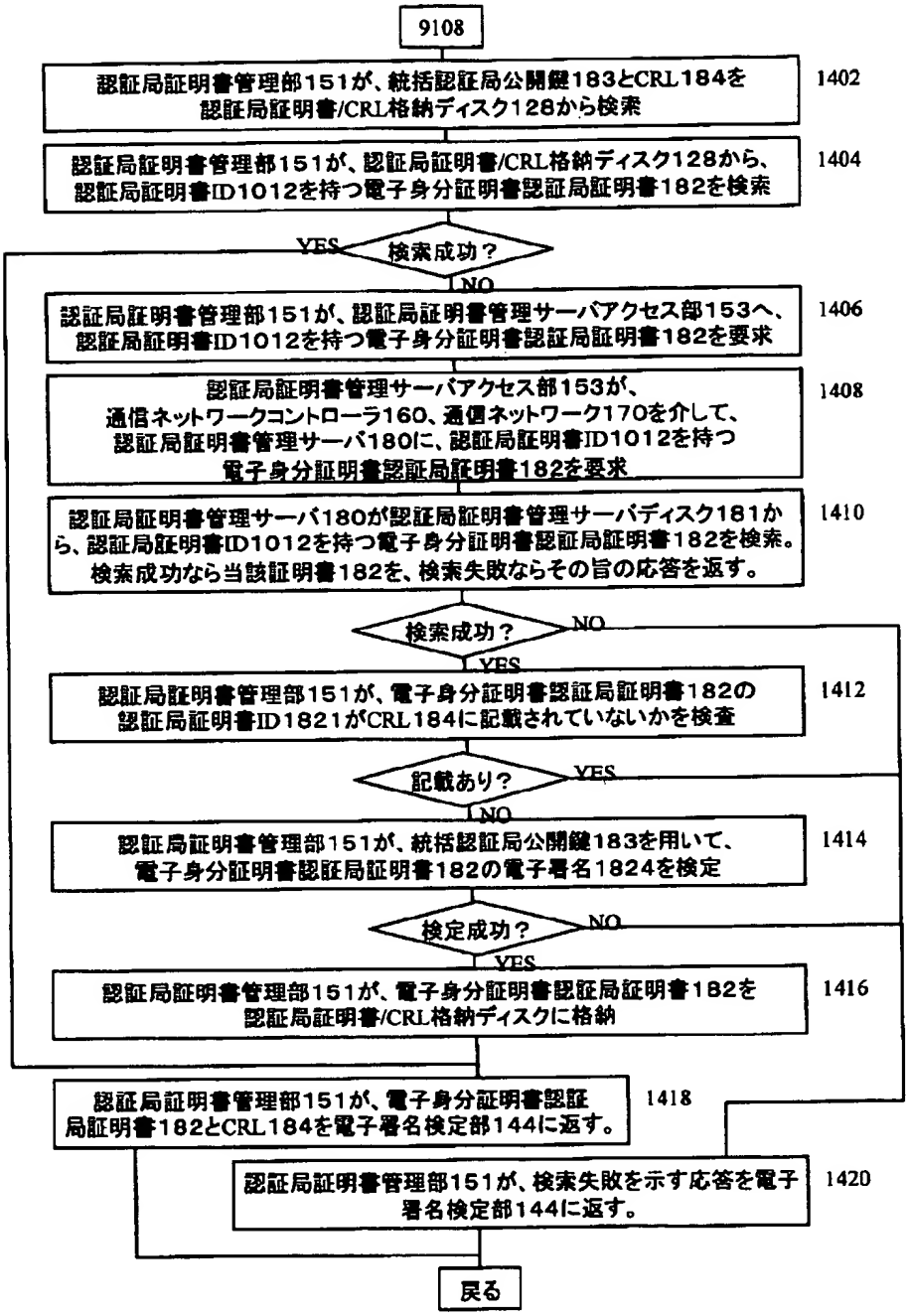
【図１３】

図13


170
通信
ネットワーク
128 認証局証明書/CRL格納ディスク
1200
電子身分証明書
確認装置
182
電子身分証明書
認証局証明書
183
統括認証局
公開鍵
184
CRL
181 認証局証明書管理サーバディスク
180
認証局証明書
管理サーバ
182
電子身分証明書
認証局証明書
184
CRL
205 電子身分証明書認証局ディスク
203
電子身分証明書
認証局
204
電子身分証明書
認証局秘密鍵
182
電子身分証明書
認証局証明書
202 統括認証局ディスク
200
統括認証局
201
統括認証局
秘密鍵
183
統括認証局
公開鍵
184
CRL

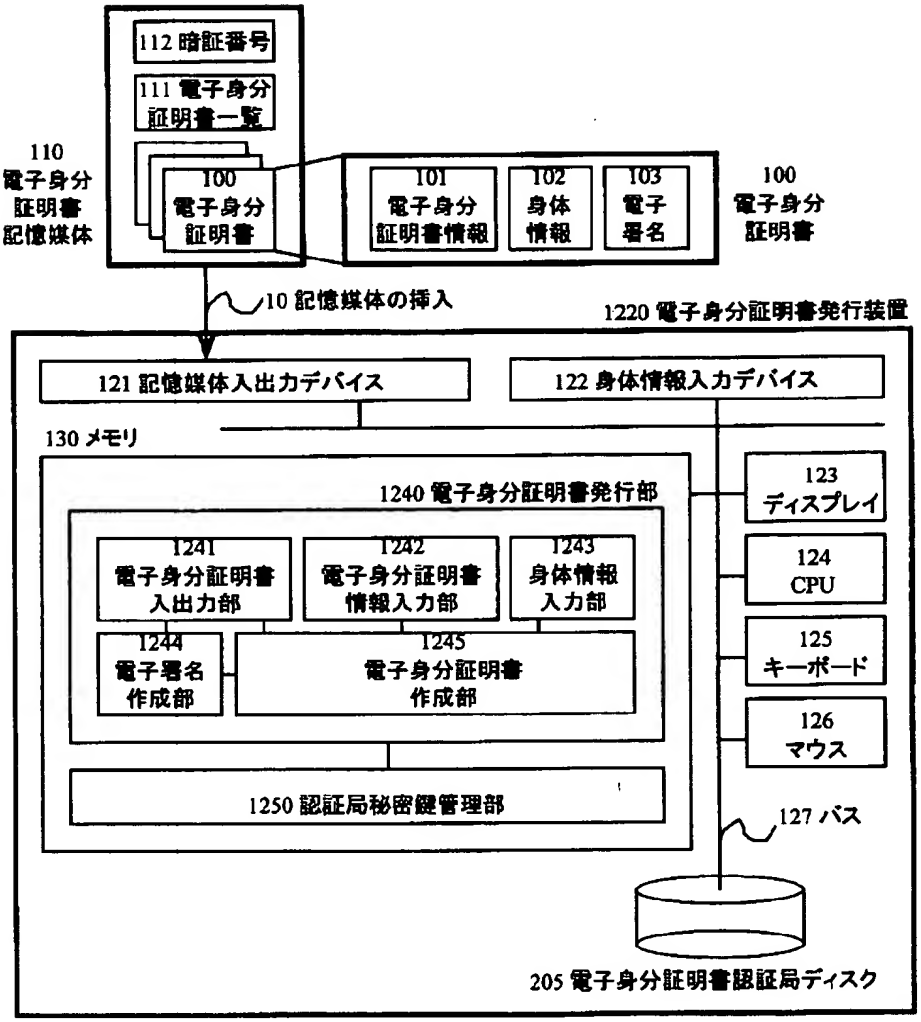
【図１４】

図14


9108
認証局証明書管理部151が、統括認証局公開鍵183とCRL184を認証局証明書/CRL格納ディスク128から検索
1402
認証局証明書管理部151が、認証局証明書/CRL格納ディスク128から、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を検索
1404
検索成功？
YES
NO
認証局証明書管理部151が、認証局証明書管理サーバアクセス部153へ、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を要求
1406
認証局証明書管理サーバアクセス部153が、通信ネットワークコントローラ160、通信ネットワーク170を介して、認証局証明書管理サーバ180に、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を要求
1408
認証局証明書管理サーバ180が認証局証明書管理サーバディスク181から、認証局証明書ID1012を持つ電子身分証明書認証局証明書182を検索。検索成功なら当該証明書182を、検索失敗ならその旨の応答を返す。
1410
検索成功？
NO
YES
認証局証明書管理部151が、電子身分証明書認証局証明書182の認証局証明書ID1821がCRL184に記載されていないかを検査
1412
記載あり？
YES
NO
認証局証明書管理部151が、統括認証局公開鍵183を用いて、電子身分証明書認証局証明書182の電子署名1824を検定
1414
検定成功？
NO
YES
認証局証明書管理部151が、電子身分証明書認証局証明書182を認証局証明書/CRL格納ディスクに格納
1416
認証局証明書管理部151が、電子身分証明書認証局証明書182とCRL184を電子署名検定部144に返す。
1418
認証局証明書管理部151が、検索失敗を示す応答を電子署名検定部144に返す。
1420
戻る

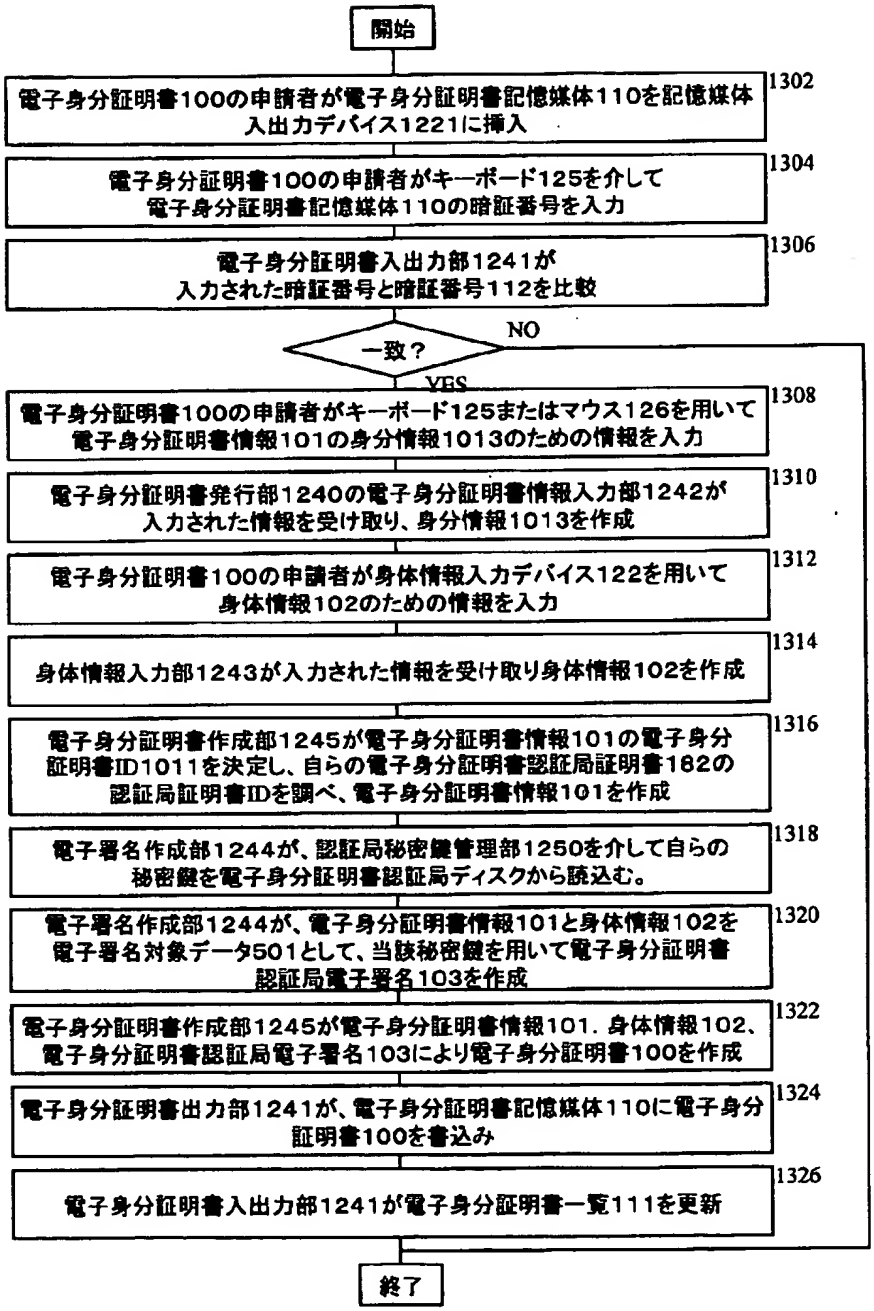
【図１５】

図15


112 暗証番号
111 電子身分証明書一覧
110 電子身分証明書記憶媒体
100 電子身分証明書
101 電子身分証明書情報
102 身体情報
103 電子署名
100 電子身分証明書
10 記憶媒体の挿入
1220 電子身分証明書発行装置
121 記憶媒体入出力デバイス
122 身体情報入力デバイス
130 メモリ
1240 電子身分証明書発行部
1241 電子身分証明書入出力部
1242 電子身分証明書情報入力部
1243 身体情報入力部
1244 電子署名作成部
1245 電子身分証明書作成部
1250 認証局秘密鍵管理部
123 ディスプレイ
124 CPU
125 キーボード
126 マウス
127 バス
205 電子身分証明書認証局ディスク

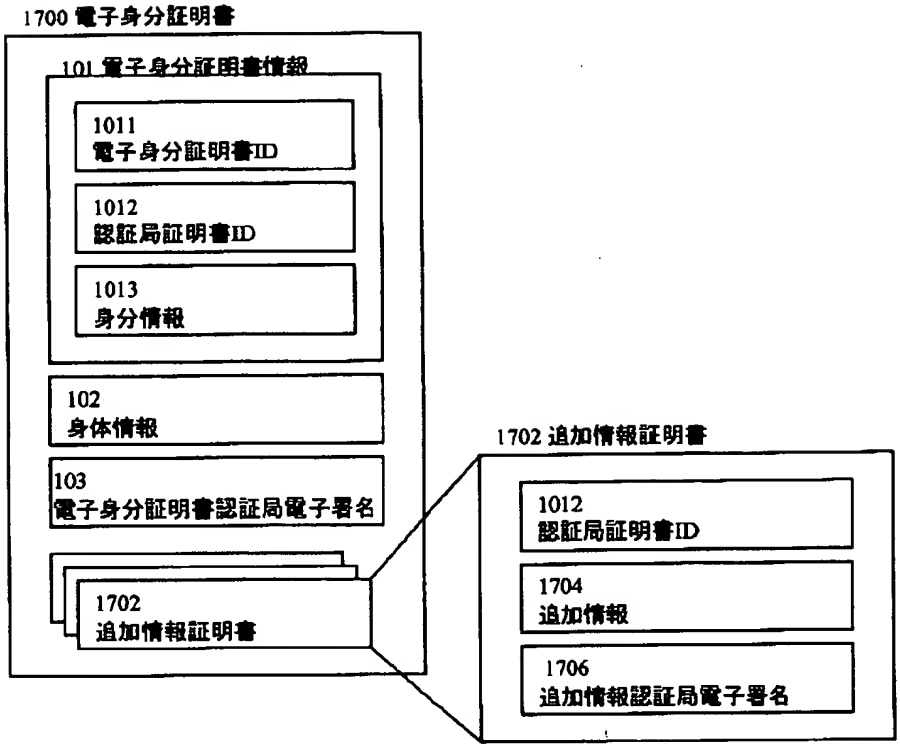
【図１６】

図16


開始
電子身分証明書100の申請者が電子身分証明書記憶媒体110を記憶媒体入出力デバイス1221に挿入
1302
電子身分証明書100の申請者がキーボード125を介して電子身分証明書記憶媒体110の暗証番号を入力
1304
電子身分証明書入出力部1241が入力された暗証番号と暗証番号112を比較
1306
一致？
NO
YES
電子身分証明書100の申請者がキーボード125またはマウス126を用いて電子身分証明書情報101の身分情報1013のための情報を入力
1308
電子身分証明書発行部1240の電子身分証明書情報入力部1242が入力された情報を受け取り、身分情報1013を作成
1310
電子身分証明書100の申請者が身体情報入力デバイス122を用いて身体情報102のための情報を入力
1312
身体情報入力部1243が入力された情報を受け取り身体情報102を作成
1314
電子身分証明書作成部1245が電子身分証明書情報101の電子身分証明書ID1011を決定し、自らの電子身分証明書認証局証明書182の認証局証明書IDを調べ、電子身分証明書情報101を作成
1316
電子署名作成部1244が、認証局秘密鍵管理部1250を介して自らの秘密鍵を電子身分証明書認証局ディスクから読込む。
1318
電子署名作成部1244が、電子身分証明書情報101と身体情報102を電子署名対象データ501として、当該秘密鍵を用いて電子身分証明書認証局電子署名103を作成
1320
電子身分証明書作成部1245が電子身分証明書情報101．身体情報102、電子身分証明書認証局電子署名103により電子身分証明書100を作成
1322
電子身分証明書出力部1241が、電子身分証明書記憶媒体110に電子身分証明書100を書込み
1324
電子身分証明書入出力部1241が電子身分証明書一覧111を更新
1326
終了

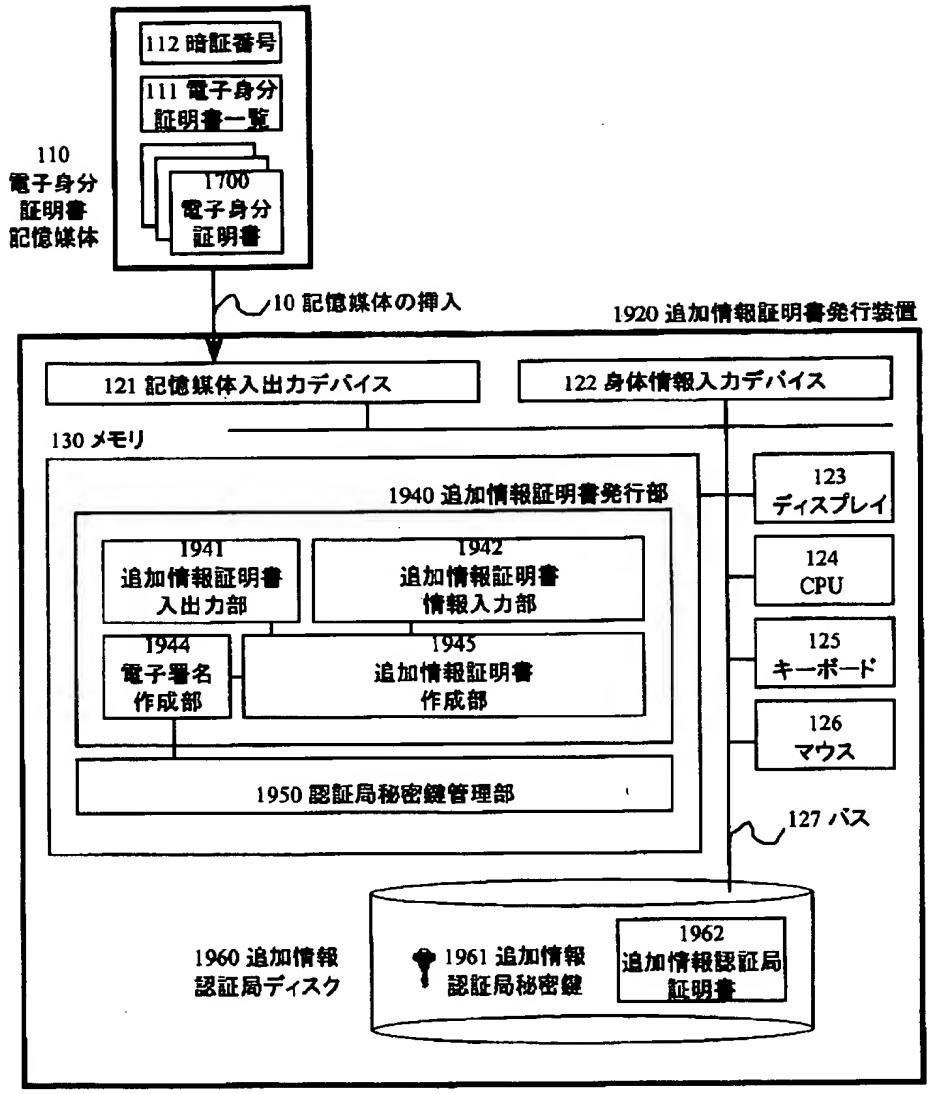
【図１７】

図17


1700 電子身分証明書
101 電子身分証明書情報
1011
電子身分証明書ID
1012
認証局証明書ID
1013
身分情報
102
身体情報
103
電子身分証明書認証局電子署名
1702
追加情報証明書
1702 追加情報証明書
1012
認証局証明書ID
1704
追加情報
1706
追加情報認証局電子署名

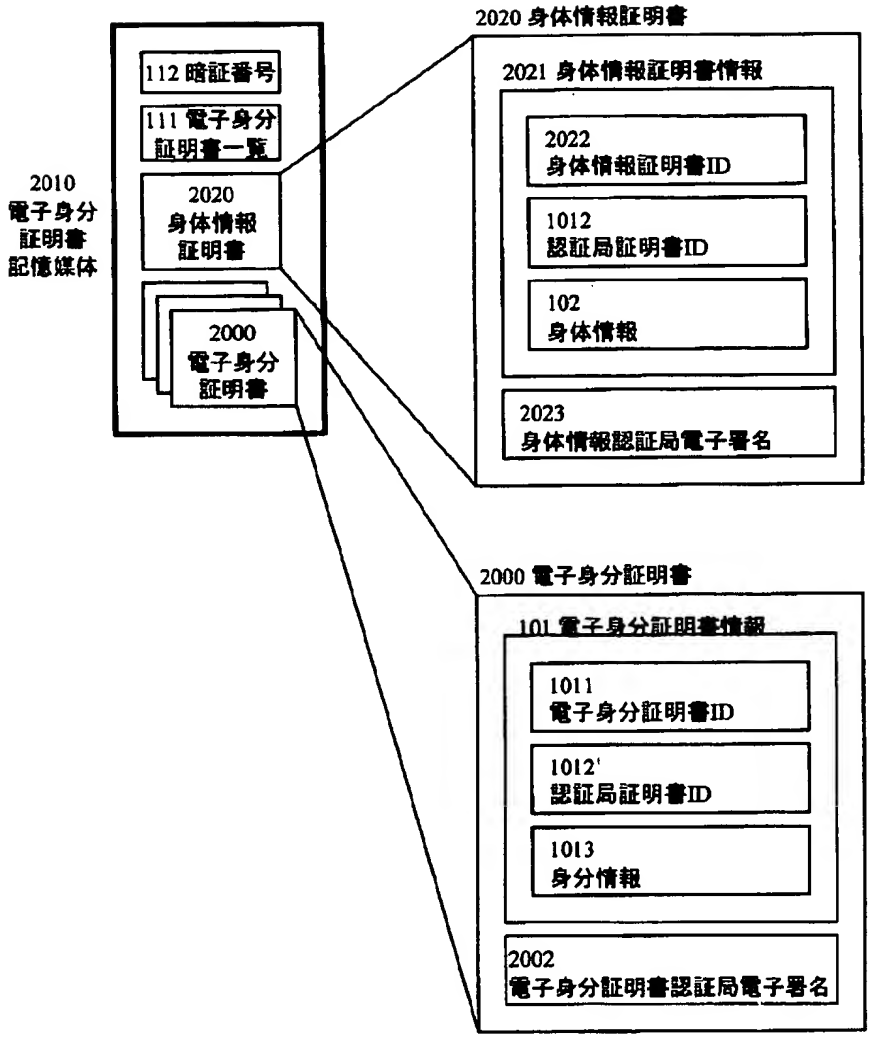
【図１８】

図18


112 暗証番号
111 電子身分証明書一覧
1700 電子身分証明書
110 電子身分証明書記憶媒体
10 記憶媒体の挿入
1920 追加情報証明書発行装置
121 記憶媒体入出力デバイス
122 身体情報入力デバイス
130 メモリ
1940 追加情報証明書発行部
1941 追加情報証明書入出力部
1942 追加情報証明書情報入力部
1944 電子署名作成部
1945 追加情報証明書作成部
1950 認証局秘密鍵管理部
123 ディスプレイ
124 CPU
125 キーボード
126 マウス
127 バス
1960 追加情報認証局ディスク
1961 追加情報認証局秘密鍵
1962 追加情報認証局証明書

【図１９】

図19


2010
電子身分
証明書
記憶媒体
112 暗証番号
111 電子身分
証明書一覧
2020
身体情報
証明書
2000
電子身分
証明書
2020 身体情報証明書
2021 身体情報証明書情報
2022
身体情報証明書ID
1012
認証局証明書ID
102
身体情報
2023
身体情報認証局電子署名
2000 電子身分証明書
101 電子身分証明書情報
1011
電子身分証明書ID
1012'
認証局証明書ID
1013
身分情報
2002
電子身分証明書認証局電子署名